ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«ҒҰМАРБЕК ДӘУКЕЕВ АТЫНДАҒЫ АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ»
коммерциялық емес акционерлік қоғамы
Ақпарттық қауіпсіздік жүйелері кафедрасы

«ҚОРҒАУҒА ЖІБЕРІЛДІ»
Кафедра меңгерушісі с.ғ.к., доцент Бердібаев Р.Ш.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «_____» _____ 2020 ж.
(қолы)

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: 5G желісіндегі ақпараттық қауіпсіздікті талдау

Мамандығы: 5В100200 – «Ақпараттық қауіпсіздік жүйелері»
Орындаған: Әли Алтынай Қуанышқызы Тобы СИБк-16-1
(аты-жөні)
Ғылыми жетекші: т.ғ.д., профессор Якубова Мубарак Захидовна
(ғылыми дәрежесі, атағы, аты-жөні)
Кеңесшілер:
Мамандығы бойынша:
аға оқытушы Дмитриева Маргарита Валерьевна
(ғылыми дәрежесі, атағы, аты-жөні)
_____«_____»_____ 2020 ж.
(қолы)
Тіршілік қауіпсіздігі бөлімі бойынша:
доцент Жандаулетова Фарида Рустембековна
(ғылыми дәрежесі, атағы, аты-жөні)
_____«_____»_____ 2020 ж.
(қолы)
Мөлшер бақылаушы:
аға оқытушы Альмуратова Камшат Бимуратовна
(ғылыми дәрежесі, атағы, аты-жөні)
_____«_____»_____ 2020 ж.
(қолы)
Пікір беруші:
Шаяхметова Асем Серикбаева
(ғылыми дәрежесі, атағы, аты-жөні)
_____«_____»_____ 2020 ж.
(қолы)

Алматы 2020

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«ҒҰМАРБЕК ДӘУКЕЕВ АТЫНДАҒЫ АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ»
коммерциялық емес акционерлік қоғамы

Басқару және ақпараттық технологиялар институты
Ақпараттық қауіпсіздік жүйелері кафедрасы
5В100200 – «Ақпараттық қауіпсіздік жүйелері» мамандығы

Дипломдық жобаны орындауға берілген
ТАПСЫРМА

Студент: Әли Алтынай Қуанышқызы
(аты-жөні)

Жобаның тақырыбы: 5G желісіндегі ақпараттық қауіпсіздікті талдау

2020 ж. «11» 11 №146 университет бұйрығымен бекітілді.

Аяқталған жұмысты тапсыру мерзімі: «____»_____20___ ж.

Жобаға алғашқы деректер (талап етілетін зерттеу (жоба) нәтижелерінің параметрлері және зерттеу нысанының алғашқы деректері):
5G желілерінде кідіріс 1 миллисекунд болады. 1 шаршы километрге 1 миллион ақылды және мобильді құрылғылар қосыла алады. Егер төртінші буын желілерінде деректерді беру жылдамдығы 100 Мбит/с болса, бесінші буынды желілерінде жылдамдық 10 есе асып, 1 Гбит/с құрауы мүмкін. 5G төртінші буын желілерінен айырмашылығы 2 жиілікте жұмыс істейді: 6 ГГц дейін және 6 ГГц жоғары. Төртінші буын желісінде сымсыз арнаның ең үлкен ені - 20МГц, ал бесінші буын желісінде 6 ГГц - ке дейінгі жиіліктер үшін - 100МГц, 6 ГГц-тен жоғары жиіліктер үшін-50-ден 400 МГц-ге дейін. 5G желісінде MIMO антеннасы қолданылады.

Диплом жобасындағы әзірленуі тиіс мәселелер тізімі немесе диплом жобасының қысқаша мазмұны:
1. 5G желісінің негіздері және жаңа буындағы ақпараттық қауіпсіздіктің қатерлері.
2. 5G желісіндегі ақпараттық қауіпсіздікті ұйымдастырудың шешімдері.

3. Жобаның тәжірибелік бөлімі. Cisco Packet Tracer симуляторында 5G желісінің прототипін жобалау.

4. Жұмыс жағдайында жерге тұйықтауды есептеу. Электр тогының адам ағзасына әсерін талдау.

5. Ақпараттық қауіпсіздік тәуекелдерін екі параметр бойынша бағалау.

Графикалық материалдардың (міндетті түрде дайындалатын сызбаларды көрсету) тізімі:

1.1 кесте - Ұялы байланыстың соңғы екі буынын салыстыру

1.2 кесте - Ұялы байланыс буындарындағы негізгі қауіптер

1.3 кесте - 5G ұялы байланыс желісіндегі шабуылдардың негізгі түрлері

2.1 кесте - 5G желісінің қауіпсіздік технологиялары

3.2 кесте - Клиенттерге берілетін IP-желілер кестесі

5.7 кесте – Екі параметр бойынша есептеулердің нәтижесі

1.1 сурет – Белсенді антенналық жүйелер мен Massive MIMO жүйелерді қолдану

1.9 сурет - 5G желісі және ықтимал қауіптер ландшафты

2.2 сурет - IPsec арнасының типтік үлгісі

Негізгі ұсынылатын әдебиеттер:

1. Omar Santos, John Stuppi. CCNA Security 210-260 Official Cert Guideб - Cisco Press, 2015

2. S. S. Vikas, K. Pawan, A. K. Gurudatt, and G. Shyam, “Mobile cloud computing: Security threats,” in 2014 International Conference on Electronics and Communication Systems (ICECS), Feb 2014

3. М.К. Дюсебаев, Т.Е. Хакимжанов, Ж.С. Абдимуратов «Еңбекті қорғау және тіршілік қауіпсіздігі»/оқу құралы. АУЭС. Алматы, 2012. -80 б.

Жоба бойынша жобаның бөлімдеріне қатысты белгіленген кеңесшілер

Бөлімдері	Кеңесшілері	Мерзімі	Қолы
Негізгі бөлім	Якубова М.З.		
Өміртішілік			
қауіпсіздігі	Жандаулетова Ф.Р.		
Тәуекелдерді есептеу			
бөлімі	Дмитриева М.В.		

Диплом жобасын дайындау
КЕСТЕСІ

Бөлімдердің атауы, әзірленетін мәселелердің тізімі	Ғылыми жетекшіге ұсыну мерзімдері	Ескерту
Кіріспе	12.02.20 – 14.02.20	орындалды
1 5G желісінің негіздері және жаңа буындағы ақпараттық қауіпсіздіктің қатерлеті	19.02.20 – 09.03.20	орындалды
1.1 5G желісінің негіздері және ұялы байланыстың алдыңғы буынымен салыстыру	19.02.20 – 29.02.20	орындалды
1.2 5G мобильді желілеріндегі негізгі қауіпсіздік мәселелері	29.02.20 – 09.03.20	орындалды
2 5G желісіндегі ақпараттық қауіпсіздікті ұйымдастырудың шешімдері	10.03.20 – 25.03.20	орындалды
2.1 5G желісінің қауіпсіздік талаптары	10.03.20 – 15.03.20	орындалды
2.2 5G желісінің қауіпсіздік шешімдері	15.03.20 – 25.03.20	орындалды
3 Тәжірибелік бөлім	01.04.20 – 10.04.20	орындалды
4 Өміртіршілік қауіпсіздігі	19.04.20 – 15.05.20	орындалды
4.1 Кәсіпорындағы еңбек жағдайларын талдау	19.04.20 – 02.05.20	орындалды
4.2 Есептеу бөлімі	02.05.20 – 15.05.20	орындалды
5 Ақпараттық қауіпсіздіктің тәуекелдерін есептеу	08.05.20 – 28.05.20	орындалды
5.1 Ақпараттық қауіпсіздік тәуекелдері	08.05.20 – 15.05.20	орындалды
5.2 Екі параметр бойынша есептеу	15.05.20 – 28.05.20	орындалды

Тапсырманың берілген уақыты «_12_»_____қаңтар_____ 2020 ж.

Кафедра меңгерушісі _____ (Бердібаев Р.Ш.)
(қолы) (аты-жөні)

Жобаның
ғылыми жетекшісі _____ (Якубова М.З.)
(қолы) (аты-жөні)

Орындалатын тапсырманы
қабылдаған студент _____ (Әли А.Қ.)
(қолы) (аты-жөні)

Аңдатпа

5G желісі ұялы байланыс технологиясының және телекоммуникация саласының жаңа қадамы. 5G жаңа мүмкіндіктерге жол ашқанымен ақпараттық қауіпсіздік жағынан мінсіз емес. Бұл дипломдық жобада 5G желісіндегі ақпараттық қауіпсіздіктің негізгі кемшіліктеріне талдау жасалынып, оларды шешу жолдары барынша сипатталды.

Дипломдық жобаның тәжірибелік бөлімінде 5G желісі жобаланды және ақпараттық қауіпсіздікті қамтамассыз ету амалдары орындалды. «Өміртіршілік қауіпсіздігі» бөлімінде жобалық қондырғысы бар аудандағы электр тогының зияндылығына негізінделген есептеулер жүргізілді. Дипломдық жобаның «Ақпараттық қауіпсіздік тәуекелдерін бағалау» бөлімінде екі параметр бойынша тәуекелдері бағаланды.

Аннотация

Сеть 5G - это новый шаг в технологии сотовой связи и отрасли телекоммуникаций. 5G не идеален в отношении информационной безопасности, тем не менее, открывает путь к новым возможностям. В данной дипломном проекте проанализированы основные недостатки информационной безопасности в сети 5G и предложены пути их решения.

В практической части дипломной работы была спроектирована сеть 5G и выполнена работа по обеспечению информационной безопасности. В разделе «Безопасность жизнедеятельности» были сделаны расчеты, основанные на вредности электрического тока в районе с проектной установкой. В разделе «Оценки рисков информационной безопасности» дипломного проекта были оценены риски по двум праматетрам.

Annotation

The 5G network is a new step in cellular communication technology and the telecommunications industry. 5G is not ideal in terms of information security, however, opening the way to new opportunities. This thesis analyzes the main disadvantages of information security in the 5G network and the ways to solve them are fully described.

In the practical part of the thesis, the 5G network was designed and the work on information security was performed. In the section Safety of life, calculations were made based on the harmfulness of electric current in the area with the design installation. In the information security risk assessment section of the diploma project, the risks were assessed by two parameters.

Мазмұны

Кіріспе

Нарықтың өсіп келе жатқан қажеттіліктеріне байланысты әртүрлі трафикті таратудың жоғары сипаттамалары бар кеңжолақты желіні ұйымдастыру мәселесі қазіргі таңда маңызды болумен қатар және мұндай жүйелердің қауіпсіздігі мәселесі өзекті болып табылады.

5G желілері – біздің заманымыздың ең үлкен жаңалықтарының бірі, бұл жалпы телекоммуникация саласын дамытудың келесі қадамы. Ұялы байланыс желілерінің осы буыны баға/сапаның ең жақсы арақатынасын қамтамасыз етуге мүмкіндік береді. Бесінші буын желісінің концептуалды тұрғысынан байланыс радиоарналары бойынша төмен кідірістерді, жоғары жылдамдықты, жоғалтудың болмауын және телекоммуникацияның неғұрлым сенімді жүйелерін қамтамасыз етуге мүмкіндік береді. Ұялы байланыстың әрбір буынының құрылуымен қызметтер одан әрі жетілдіріледі. Бүгін біз 4G ұялы байланысы деректерді де, IP негізіндегі дауысты да таратуға қабілетті екенін білеміз,бірақ 5G желісі мүмкіндіктері әлде кайда көбірек. 5G жақсартылған сипаттамалары мен бір жерден көп қосылымды қамтамассыз ете алу арқасында ақылды IoT жүйелерін дамытуға бастама береді, бұл 5G желілерінің осы жылдам өсіп келе жатқан салада маңыздылығын көрсетеді.

Біз көріп отырғанымыздай, 5G өз ізашарларынан әлдеқайда асып түседі, бірақ қауіпсіздік талаптары да сәйкесінше айтарлықтай өсіп келеді. 5G мәліметтердің кез келген түрінің және жалпы ұялы байланыс жүйесін қауіпсіздігін қамтамасыз ету үшін функционалы бар. 5G желісінде рұқсат етілмеген бұзудан, байланыс жүйесіне түрлі шабуылдардан, соның ішінде DDOS-шабуылдардан қауіпсіздік талаптарын арттыру үшін байланыс жүйелерін сенімді қорғау қажет. Кибер қылмыскерлер тарапынан жасалған шабуылдардан болған барлық қауіп-қатерлер кез келген байланыс жүйесін бас тартуға дейін жеткізуі мүмкін. Оның үстіне жаһандық деңгейдегі ұялы байланыс жүйесі үшін мұндай деңгейдегі шабуылдар өте қауіпті. 5G-дің кез келген шабуыл түрлерімен күресу үшін барлық функционалы бар. Дипломдық жобада мен бесінші буын желісіндегі мәліметтердің қауіпсіздік негіздерін, шабуыл түрлерін, қауіпсіздік архитектурасын және жаңа буынды ұялы байланыс жүйесіне шабуылдан қорғау шараларын егжей-тегжейлі зерттеуден өткіземіз және толық талдау жасаймыз.

1 5G желісінің негіздері және жаңа буындағы ақпараттық қауіпсіздіктің қатерлері

1.1 5G желісінің негіздері және ұялы байланыстың алдыңғы буындарымен салыстыру

Бесінші буын желісі ұялы байланыс желілерінің төртінші буынын алмастыруда және жылдамдық, кідіріс, қосылған құрылғылар саны сияқты көптеген сипаттамалар жақсарады. Желіні жабу және сенімділік жаңа деңгейге шықты.

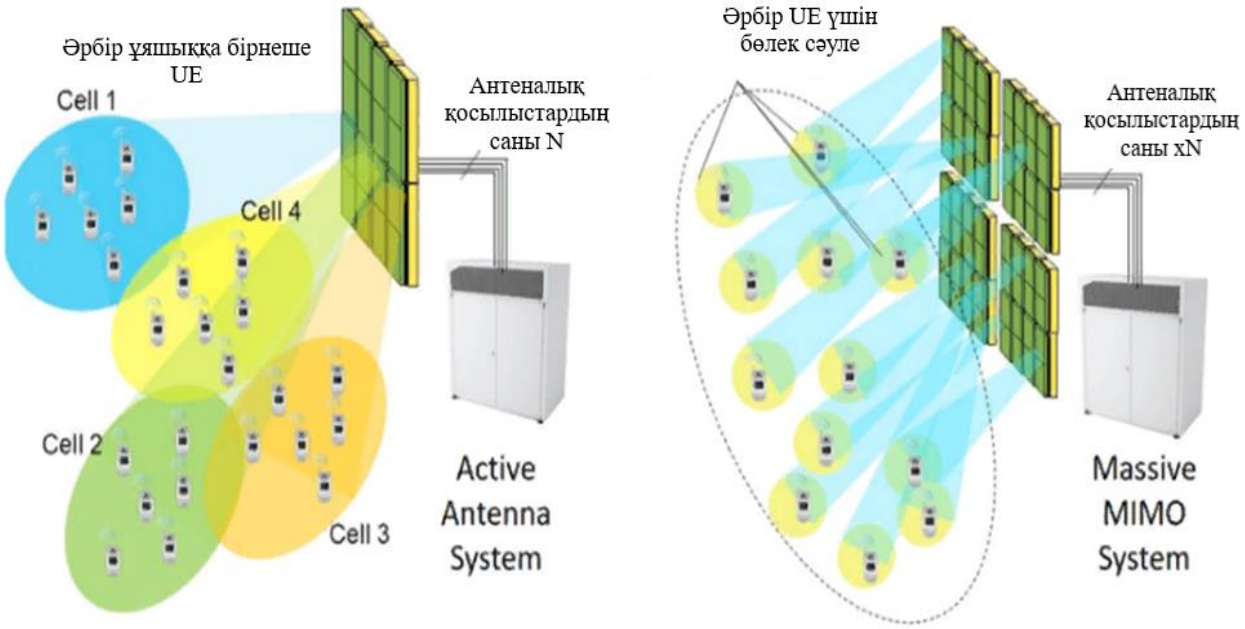
Мобильді құрылғылар санының өсуіне байланысты, алдыңғы нұсқалармен салыстырғанда желілерді жетілдіру қажет. Ұялы байланыстың алдыңғы буындардың өткізу қабілеті IoT сияқты ақылды жүйелердің жұмысы үшін жеткіліксіз, сондай-ақ интернет функционалының дамуымен мобильді құрылғылардың желілік өткізу қабілетін арттыру қажет.

5G-да басқа жиіліктер мен басқа қабылдағыш құрылғылар қолданылады. Бұл жаңашылдықтар радиоқолжетімділік бойынша құрылғылардың бірнеше есе көп қосылуына мүмкіндік береді, кідірістер минимумға дейін төмендейді, жылдамдық еселеп өседі. Егер бар тіркелген байланыс 1000 км қашықтықта кідіріс 20 миллисекунд болса, онда бесінші буын желілерінде олар тек 1 миллисекунд болады. 1 шаршы километрге 1 миллион ақылды және мобильді құрылғылар қосыла алады. Егер төртінші буын желілерінде деректерді беру жылдамдығы 100 Мбит/с болса, бесінші буынды желілерінде жылдамдық 10 есе асып, 1 Гбит/с құрауы мүмкін [1].

3GPP TS 38.211 V1.2.0 (2017-11) спецификациясына сәйкес 5G төртінші буын желілерінен айырмашылығы 2 жиілікте жұмыс істейді: 6 ГГц дейін және 6 ГГц жоғары. Төртінші буын желісінде сымсыз арнаның ең үлкен ені - 20МГц, ал бесінші буын желісінде 6 ГГц - ке дейінгі жиіліктер үшін - 100МГц, 6 ГГц-тен жоғары жиіліктер үшін-50-ден 400 МГц-ге дейін [5].

5G желісінде MIMO антеннасы қолданылады. AAS MIMO антеннансы желіні жабу аймағын белгілі бір бөліктерге бөлуге мүмкіндік береді, осының есебінен радиоспектр әлдеқайда тиімдірек пайдаланылады және бұл радиоарналарды арттыруға ықпал етеді. Бесінші буын байланыс жүйесінде миллиметрлік толқындарды қолдану тиімді. Қысқа толқынды диапазонды қолдану арқасында бағыттылық көрсеткіштері айтарлықтай жақсарады. Желілердің осы буынында антенна элементтері бір базалық станцияға ұлғаяды. Антенна элементтерінің көп саны Massive MIMO-ға қосылады. Осылайша, Massive MIMO қолданудың келесі көрсетілгендей артықшылықтары бар:

- интерференцияға байланыста мәселелер болмайды;
- базалық станцияға бағытталған ұялы байланыс радиоарналарының саны айтарлықтай көбейеді;
- сигнал-шу қатынасы ұлғаяды, бұл қабылдау құрылғысының сезімталдығының артатынын білдіреді;
- ұялы құрылғыларға шығу сигналы жеткілікті дәрежеде қуатты болады.



1.1 сурет – Белсенді антенналық жүйелер мен Massive MIMO жүйелерді қолдану

Ұялы байланыс станциясынан мобильді станцияға жіберілген SRS-пакет сымсыз арнаның сапасын тексеруге мүмкіндік береді. Соңғы мобильді құрылғылар осы пакетті тарата алады және сапасын тек өзінің таратушы антеннасы арқылы ғана тексереді. Осы арқылы ұялы байланыс станциясы тек соңғы құрылғы үшін радиоарнаның сапасын тексереді. 5G-да барлық арналардың сапасын тексеру үшін таратқышты таңдау технологиясы бар. Осы технологияның арқасында станциядан жоғары сапалы ұялы құрылғы бағытында дәл сәуле қалыптасады. Бұл жаңа буындардың байланыс жүйесінде байланыс арналарының өткізу қабілетін арттырады.

Бесінші буын желілерінде бір-бірінен тәуелсіз желі құру мүмкіндігі бар, бұл заңды тұлғалардың көп санын қосуға және "ақылды заттарды" дамытуға мүмкіндік береді. Электрмен жабдықтау, көлік құралдары арасындағы байланыс, денсаулық сақтау, банк құрылымы сияқты "ақылды жүйелерді" құру үшін барлық мүмкіндіктер пайда болды.

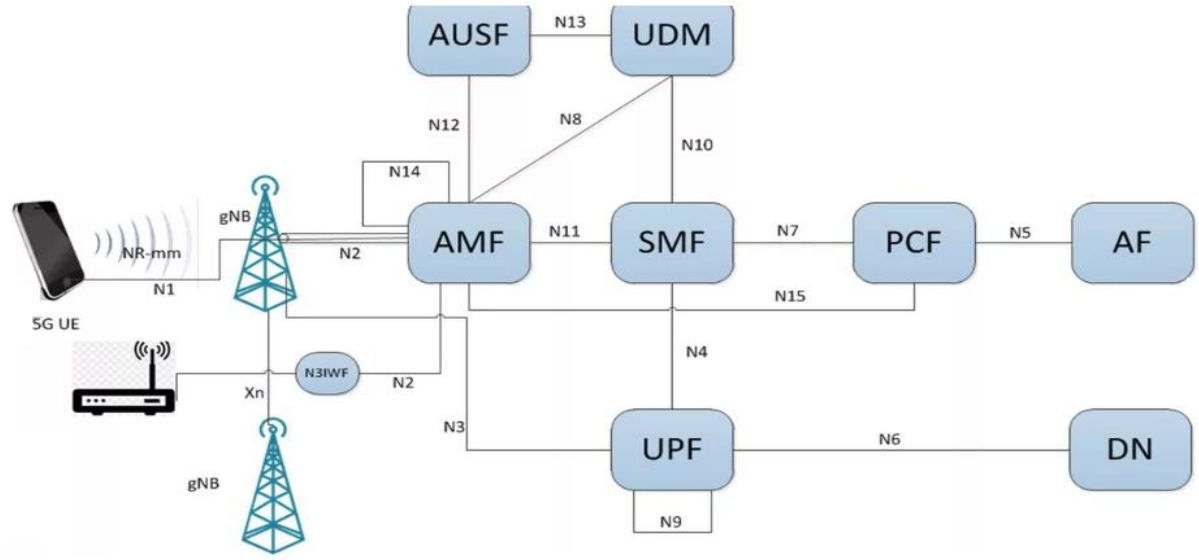
1.1 кесте - Ұялы байланыстың соңғы екі буынын салыстыру [5]

Желі параметрлері	4G	5G
Жылдамдық сипаттамалары	1000 Мбит/с дейін	20000 Мбит/с дейін
Соңғы құрылғылар	Ұялы телефондар, сымсыз құрылғылар	IoT, IP TV, ұялы жүйелер, сымсыз құрылғылар
1 км^2 қосылыстар саны	1000-10000	1 миллион
Жұмыс істеу	LTE-Advanced, WiMax	IMT-2020

технологиясы	Release 2 (IEEE 802.16m)	
Жаңа қызметтер	Интернетке жылдам шығу, мультимедианы қолдау	IoT, IPTV, 3D, UHD, HD бейне жүйелері
Ұялы байланыс желісіндегі кідіріс деңгейі	10-100мс	1мс

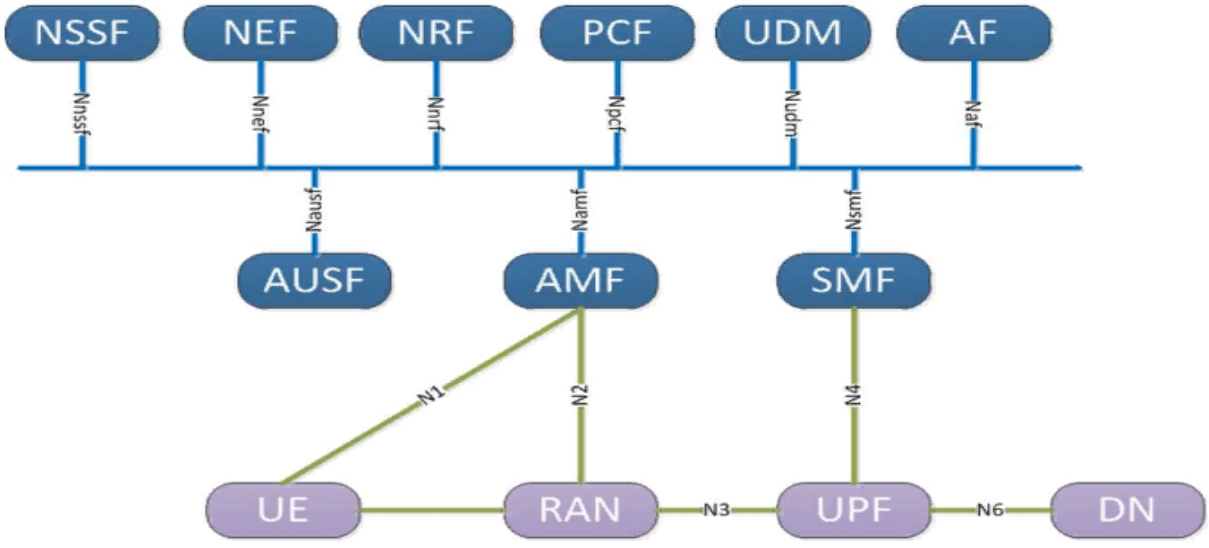
Бесінші буын желілерінің архитектурасы ядро желісін, желіаралық бөлікті, көлік желісін және радиоқатынау желісін қамтиды.

1.2 суретте бесінші буын желісінің архитектурасы және барлық модульдер мен функциялар арасындағы байланыс көрсетілген.



1.2 сурет – 5G желісінің архитектурасы және желілік модульдердің өзара қарым-қатынасының жүйелілігі

1.3 суретте 5G желісінің интерфейстерінің көрнекілігі үшін басқа түрдегі архитектура көрсетілген.



1.3 сурет – 5G желісінің архитектурасы және желілік интерфейстері

Бесінші буын ұялы байланыс желісіндегі әрбір модульдің функциясына түсініктеме берейік:

- AMF – құрылғыны базалық станцияға қосқан кезде қатынауды бақылау, сондай-ақ мобильді басқару функциясы;
- SMF – белсенді белгіленген сессияларды бақылау функциясы;
- UPF – 5G ұялы желісінде қолданушылар деректерін сенімді жеткізу үшін жауап береді;
- UDM – абоненттердің пайдалы және қызметтік деректерін басқаруға жауап беретін функция;
- UDR – қызметтік ақпарат сақталатын деректер базасы;
- PCF – бұл модуль соңғы буын желілеріндегі политиканы басқаруды жүзеге асырады;
- AF – қосымша немесе қолданбалы ұялы байланыс модулі;
- NSSF – желі қабатын анықтау модулі;
- PCF- 5G байланыс желісіндегі ережелерді басқару модулі;
- NEF – басқа қосымшалармен байланысты бақылауға арналған модуль;
- NRF – барлық желілік функционал сақталатын модуль;
- SMSF – NAS хаттамасының көмегімен SMS қабылдау/жіберу үшін жауап береді.

5G желісін жаппай пайдалануға енгізгеннен кейін "ақылды" үйлердің, кеңселердің және тіпті қалалардың жүйесін құру дамитын болады. Бұл барлық автоматтандырылған байланыс жүйелерін қашықтықтан басқаруды бірнеше рет жеңілдетеді. 4G желісімен салыстырғанда трафик деңгейі 10 есе артуы мүмкін. Желідегі проблемаларды диагностикалау мен жою бірнеше рет жеңілдетіледі және енді көптеген мәселелер қысқа мерзімде және кідіріссіз шешілетін болады.

Ағындық бейне саласында да жаппай өзгерістер күтілуде. Енді теледидарға арналған STB-қосымша құралы мен шлюздерді пайдалану екінші жоспарға кетеді. Басымдықта сымсыз контенттік бейне пайда болады, орналасу орны бойынша шектеулер жойылады. Аз кідіріс және деректерді берудің жоғары жылдамдығына байланысты, бейнетрансляция бейненің жоғары сапасымен жиірек өткізіледі. Осылайша, 4К бейне сапасымен трансляция жүргізу мүмкіндігі пайда болады, ал бұл мультикаст трафигін тарату саласында үлкен серпіліс.

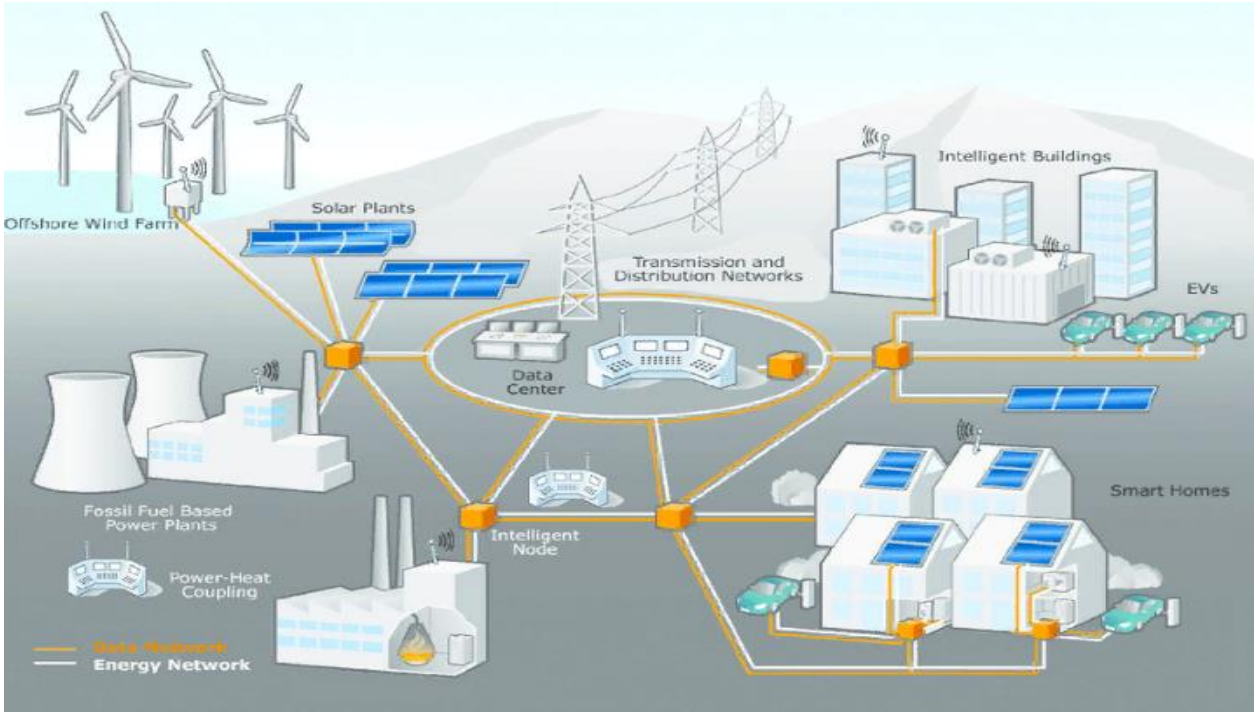
IoT-ты жаппай дамыту үшін ақпарат беру жылдамдығы мен сенімділігі, желідегі барлық сегменттер арасындағы төмен кідірістер сияқты параметрлер өте маңызды. "Ақылды заттарды" құру үшін электр тұтыну төмен болуы тиіс, өйткені бір базалық станцияға қосылымдардың саны көп болуы мүмкін және бұл электр энергиясының шығындары есе артуын тудырады. 5G мұндай байланыс жүйелерін құруды қамтамасыз ете алады, себебі деректерді беру жылдамдығы барлық алдыңғы шешімдерден 10 есе артық болады, кідірістер 90% - ға азаяды және 1км^2-ге қосылу саны 1 миллионға жетуі мүмкін.

Ұялы байланыстың бесінші буынының желілері базалық станцияның радио интерфейсі арқылы өзара барлық автоматтандырылған процестердің өзара әрекеттесуінің үлкен инфрақұрылымын құруға арналған [2].

Бесінші буын желісі VANET желісін өрістетуге және жол қозғалысын сенімді байланыс жүйелерімен қамтамасыз етуге мүмкіндік береді, бұл ЖКО саны бірнеше есе қысқаратын сенімді жол қозғалысын қамтамасыз етуге мүмкіндік береді.

5G желілерінің мониторингі де жеңілдетіледі, енді бүкіл инфрақұрылымды тәулік бойы қарауға болады және барлық оқиға ашық орын алады.

Huawei компаниясы 5G қолдауымен ұялы телефондарды белсенді түрде шығаруда.



1.4 сурет –5G негізіндегі IoT желісі

1.2 Алдыңғы буындардың ақпараттық қауіпсіздік жүйелері және оларды салыстыру

1G ұялы байланыстың бірінші буыны болды. Ол толық аналогты телефон байланысымен ұсынылды. Қауіпсіздік тұрғысынан бірінші буын шабуылдардан жеткілікті қорғалмаған және аналогтық байланыс жүйелерінің жаппай бұзылуына әкеп соқты. Қаскүнемдердің алаяқтық әрекетіне байланысты операторларға да, абоненттерге да үлкен залал келтірілген. Аналогтық телефондардың тыңдауға сезімталдығы өте төмен болды, зиянкестер мен ұялы байланыс провайдерлері үлкен шығындарға ұшырады.

2G GSM желілерінің пайда болуымен және сандық мобильді байланысқа көшумен қауіпсіздік функциялары айтарлықтай кеңейді. Тәжірибе ретінде бірінші буын желісі мен аналогтық байланыс шабуылдары қызмет етті, сондай-ақ жаңа талаптар мен тәуекелдер ескерілді. GSM-де көбінесе дауыстық

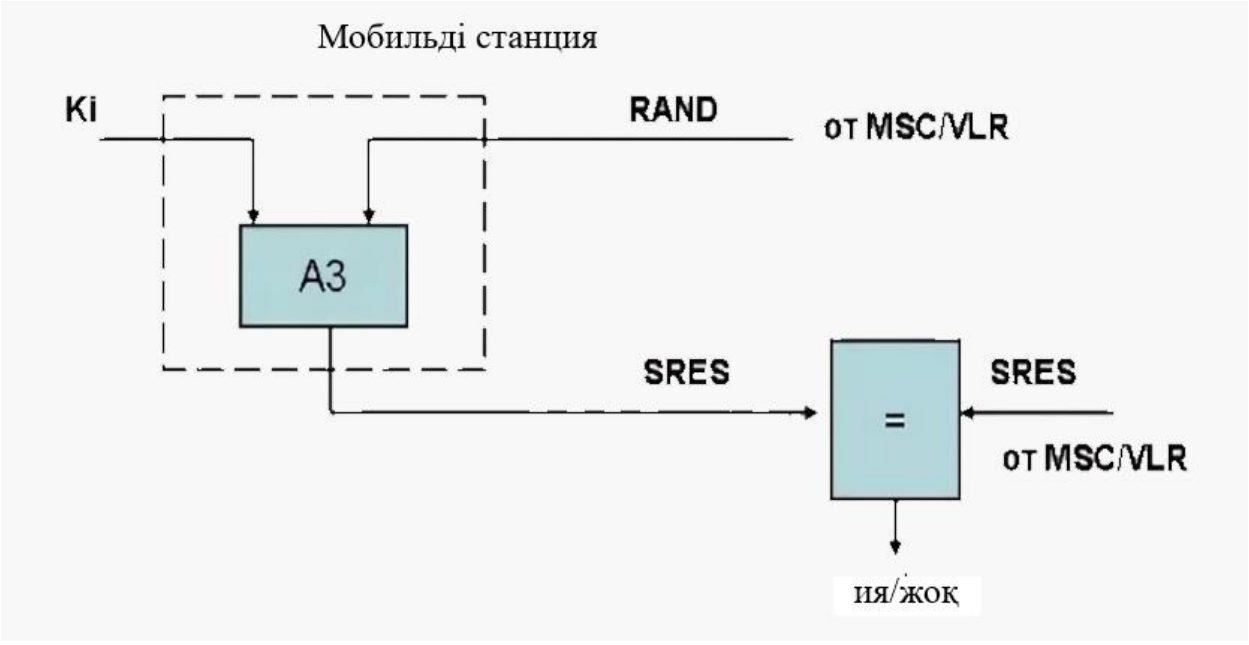
деректер, SMS және MMS беріледі және интернет желісіндегі деректер аз жылдамдықпен жіберілді.

2G желісіне шабуыл жасаудың негізгі нұсқалары SMS және MMS-ті ұстап алу, сөйлесулерді тыңдау және жазу, жеке мақсатта пайдалану үшін SIM-картаны бұзу және ұстап алу, фродтық қоңыраулар болып табылады. Бұл проблемаларды шешу және зиянкестерден қорғану үшін берілетін ақпаратты аутентификациялау, авторизациялау, шифрлеу қажет болды.

Бастапқы қорғаныспен SIM картаны қамтамасыз ету керек. SIM картаны бастапқы қорғау PIN кодымен қамтамасыз етіледі, ал арнайы функцияларды қорғау PIN2 арқасында қамтамасыз етіледі. Егер PIN сәтті енгізілсе, пайдаланушы рұқсат алады, ал 3 рет қате енгізілсе, SIM картасы бұғатталып, тек PUK кодымен құлпын ашуға болады. Осы функцияның арқасында зиянкес SIM-картаны пайдалануды қиындатады.

Шынайылықты тексеру VLR қонақ регистрінің негізі бойынша басталады. Бұл регистр Rand санының кездейсоқ жиынтығын қалыптастырады және оны абоненттің құрылғысына береді. SIM-картада Ki арнайы кілті қалыптасады, ол ешкімге белгісіз және оны ешкім оқымауға тиіс.

Қонақ регистрі аутентификация орталығына сұрау жібереді, аутентификация орталығына жауап ретінде RAND, SRES, Kc жібереді. SRES A3 алгоритмі негізінде Ki және RAND базасында, ал Kc (сымсыз арнаны шифрлеу кілті) - A8 негізінде есептеледі. Ki кілтін қолдану және оны есептеу аутентификация орталығы тарапынан, SIM картасының ішінде жүргізіледі. Ki құпия кілті шифрланған түрде аутентификация серверіне беріледі, сондықтан бұл кілтті қаскүнем іс жүзінде ала алмайды. Ұялы байланыстың 2 буыны желісіндегі абоненттердің түпнұсқалығын тексеру рәсімі басқа нөмірлерге, сырттан келген қоңырауларға, деректерді беруге және ұялы байланыс желісінде пайдаланушы құрылғыларды тіркеуге қоңырау шалу кезінде өтеді [10].



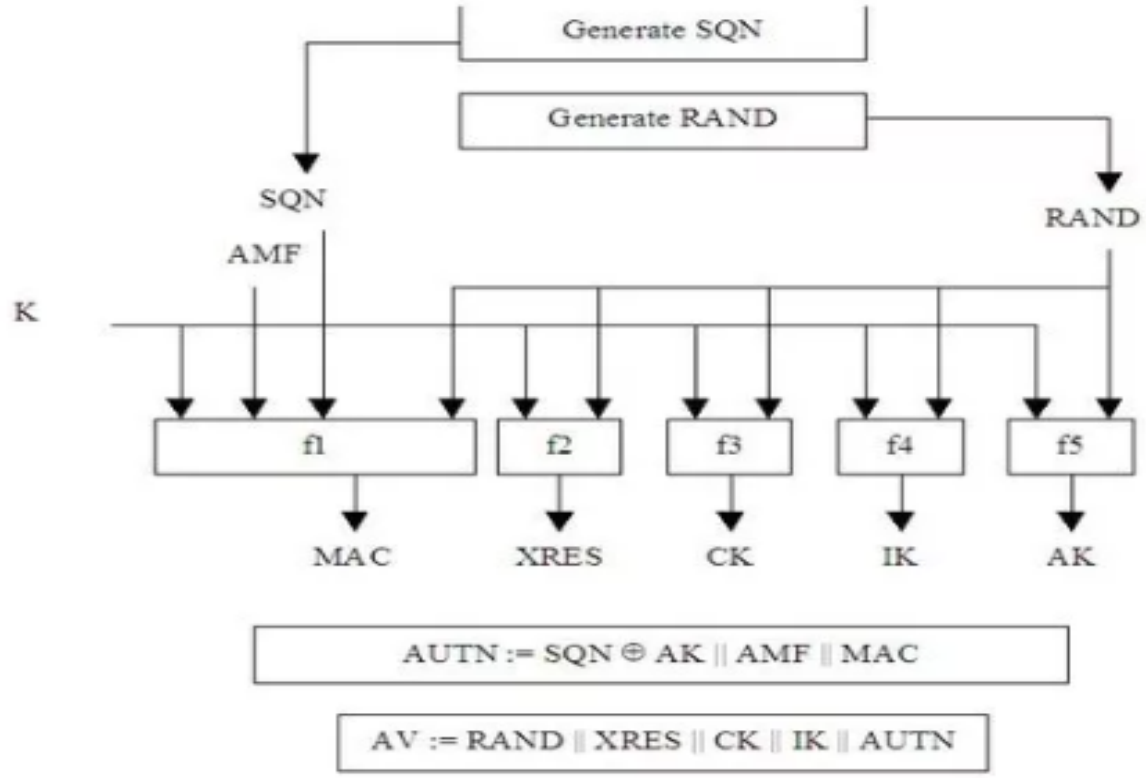
1.5 сурет – Шифрлау және аутентификация процесі

Тыңдаудан жоғары қорғаныс үшін A5 алгоритмі бойынша Кс кілтін қолдана отырып, радиоарна арқылы берілетін деректерді шифрлау қолданылады. Кс құпия кілтінің генерациясы түпнұсқалығын тексеруді жүзеге асыру процесінде жүреді. Құпия кілтті есептеу аутентификация орталығында жүреді және оның қонақ регистрі беріледі. A5 алгоритмінде 64 бит сыйымдылығы бар Кс кілті және шифрлау сөздерін есептеу үшін 22 бит сыйымдылығы бар TDMA кадр нөмірі қолданылады. Ұялы байланыс желісіндегі әрбір абонентке уақытша TMSI идентификаторы беріледі, ол да үнемі өзгеріп отырады. Енді IMSI сымсыз арна арқылы базалық станцияға дейін тасымалдау қажет емес. Осыған байланысты абонентті идентификациялау және локализацияны анықтау қиынға соғады.

3 буынды желілер пакеттік деректер базасында құрылады. Осы буынның желілерінде жаңа қауіптер пайда болды. Оларға хабарламаларды ұстап қалуды, мобильді байланыс операторларының есебінен сервисті алу үшін бүркемелеуді, маңызды ақпаратты бұзу мен таралуын, қызмет көрсетуге рұқсатсыз қол жеткізуді, байланыс жүйелерін бұзу үшін пайдаланушының немесе желі учаскесінің атынан бүркемеленуді жатқызуға болады.

UMTS желісіндегі пайдаланушылардың орнын қорғау үшін P-TMSI қолданылады. Байланыс орнатылғанда, осы ішкі пайдаланушы құрылғысының идентификаторымен ұялы байланыс желісінде алмасу орын алады.

Жүйені бүркемелеу мен бұзудан қорғау үшін өзара аутентификация қолданылады. Аутентификация орталығы және USIM картасы пайдаланушы құрылғысының кілтінің көшірмесі бойынша қамтылған, осылайша пайдаланушы құрылғысының ұялы байланыс желісімен байланысы болады. Ұялы байланыс желісінде аутентификация орталығы N аутентификациялық векторлармен кесте құрайды. Бір вектордағы компоненттер саны беске тең: RAND, XRES жауабы, Ck және Ik шифрлау кілттері, AUTH аутентификация маркері. Қонақ регистрі k аутентификационный векторын, RAND пен сәйкестендіру маркер таңдайды және AUTH абонентке жібереді. SIM картасы аутентификация маркерінің дұрыстығын тексереді. Егер тексеру сәтті болса, генерацияланады және RES желісіне жібереді. Осы параметр келіп түскеннен кейін ұялы байланыс желісінде XRES салыстыру жүргізіледі. Осылайша, желі мен мобильді құрылғы арасында байланыс орнатылады. Өзара аутентификацияның арқасында шифрлеу орындалады және деректер тұтастыққа тексеріледі. Тұтастық және шифрлау алгоритмдері-UIA / UIA [11].

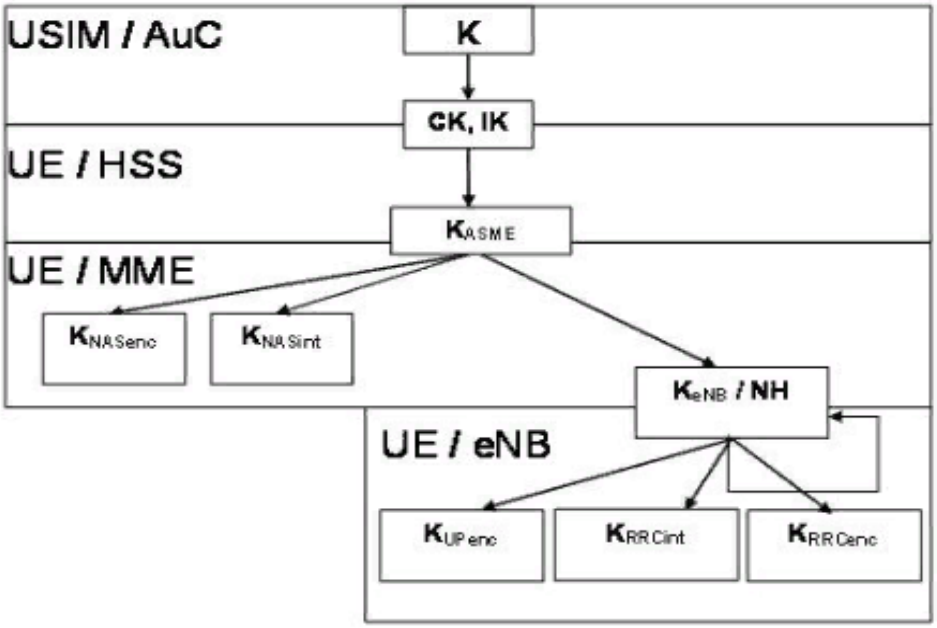


1.6 сурет – 3G желісіндегі кілттерді аутентификациялау және генерациялау процесі

4 буын желісінде үлкен өзгерістер көрсетілді. Деректерді беру жылдамдығы айтарлықтай өсті, ал қосылымдар саны артты. Желі IP, Ethernet базасында толық жұмыс істеді. Үлкен функционал мен үздік сипаттамалардың дамуымен, сондай-ақ пайдаланушылар үшін де, ұялы байланыс операторлары желісі үшін де жаңа қауіптер де пайда болды. Алаяқтық мақсатында сессия құру, IP пайдаланушылық және қызметтік пакеттерін ұстап қалу, оператор мен абоненттерге байланыс жүйелерін бас тартуға дейін жеткізу мақсатында DOS-шабуылдар сияқты қауіп-қатерлер пайда болды.

4G қауіп-қатерден қорғау үшін ағындық шифрлау қолданылады. Ашық деректерге жалған кездейсоқ деректер қойылады. Деректерді қауіпсіз беру үшін туннелдеу қолданылады. АКА аутентификация процесін іске қосады, бұл абоненттің SIM картасы мен тіркеу орталығы арасында шифрланған хабарламалармен алмасуды қамтамасыз етеді, бұл процесс секунд ішінде жүреді. Осы буын желісінде 3G сияқты USIM мен AuC арасында құпия кілттер бөлінеді. Аутентификация процесінде абонент желісі және ұялы байланыс арасында деректерді қорғау және жалпы қауіпсіздік үшін шифрлау кілттерді (Ck және Ik) құрылады. USIM-ден бұл кілттер пайдаланушы құрылғысына жіберіледі. Ал аутентификация орталығынан кілттер тіркеу орталығына жіберіледі. Содан кейін қос тарап, пайдаланушы және тіркеу орталығы негізгі жұп негізінде K_{ASME} кілтін жасайды. Осыдан кейін генерацияланған кілттің 4 буынды ұялы байланыс желісінің ID-нен тәуелділігін анықтау және оны тіркеу орталығынан ағымдағы ұялы байланыс желісінің мобильдік басқару

құрылғысына беру үдерісі жүргізіледі. K_{ASME} генерацияланған кілтінің негізінде NAS хаттамасы бойынша мобильді құрылғы мен ұялы байланысты басқару құрылғысы арасында ақпаратты шифрлеуге арналға $K_{nas\text{-}enc}$ кілті және деректер желісіне берілетін мәліметтердің тұтастығын қамтамасыз етуге арналған $K_{nas\text{-}int}$ кілті қалыптасады. Мобильді құрылғыны мобильді басқару құрылғысына қосу арқылы базалық станцияны тасымалдау үшін K_{eNB} кілтін жасау процесі басталады. Сонымен қатар, базалық станцияға толық пайдаланушы деректер берілуі үшін U-Plane хаттамасы бойынша $K_{up\text{-}enc}$ және RRC хаттамасы бойынша $K_{rrc\text{-}enc}$ кілттерімен шифрлау жүргізіледі. Барлық деректерді трафик жүру жолында шығынсыз жіберу үшін $K_{rrc\text{-}int}$ кілті жасалады.



1.7 сурет - 4G желісіндегі кілттердің иерархиясы

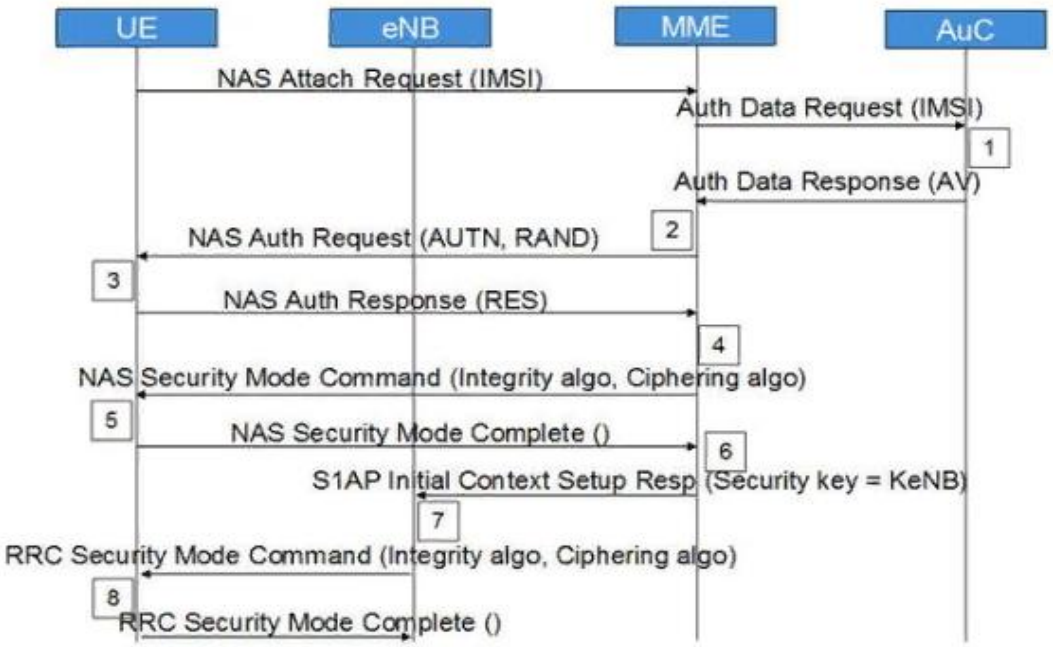
Аутентификация векторлары есептеу тек бір жаққа ғана болатын функциялардың көмегімен криптография алгоритмі негізінде құрылады. Векторларды генерациялау алгоритмі үшін 128 биттік кездейсоқ RAND саны, сыйымдылығы 128 бит бар шебер кілт және реттік нөмірлер есептегіші қолданылады. SQN есептеуіші әр түрлі және барлық жаңа аутентификация векторларын генерациялау мүмкіндігін ашады. Векторға аутентификация процесін бақылайтын AMF да кіреді. Функцияның шығуында MAC (аутентификация коды хабары) - 64 бит, Ck шифрлау кілті, Ik және АК - 64 бит бүтіндік кілті аламыз [12].

4 буын желісінде пайдаланушы құрылғысына қызмет көрсету кезінде Ck және Ik кілттері ашық берілмейді, KDF алгоритмі арқылы K_{ASME} генерациясы жүзеге асырылады. Кіріс параметрлері CK және IK. Генерациядан кейін вектор RAND, SRES, AUTN және K_{ASME} болады. Оның негізінде шифрлеу және бүтіндігін тексеру жүзеге асырылады.

Пайдаланушы құрылғысы ұялы байланыс желісінен RAND, AUTN және KSI_{ASME} параметрлерін алады. Алынған USIM параметрлерінің негізінде XMAC, RES, CK және IK есептеу басталады. Содан кейін соңғы пайдаланушы

есептелген RES таратады және оны ұялы байланыс басқару құрылғысына жібереді, онда алынған деректер салыстырылады. МАК құрылғысында есептелген ХМАК -мен салыстырылады. Егер барлық салыстырулар сәтті болса, бұл аутентификация сәтті өтті және одан әрі ядро, базалық станция және мобильді құрылғы желісі арасында алмасу орын алады [12].

Деректерді шифрлау және олардың бүтіндігін тексеру үшін UEA2, UIA2, AES, DES қолданылады.



1.8 сурет - Аутентификация және шифрлау процесі

Енді ұялы байланыстың 3 буынына салыстырмалы сипаттама береміз. Салыстыру негізінде біз осалдықтардың өзгеру динамикасын және ұялы байланыс желілері үшін жаңа қауіптерді көреміз.

1.2 кесте - Ұялы байланыс буындарындағы негізгі қауіптер

№	2G	3G	4G
1	SIM картасын бұзу	Жалған базалық станцияны пайдалану	Алаяқтық мақсатында сессия құру
2	Сөйлесулерді жазу	Жабдыққа қол жеткізу үшін бүркемелеу	DOS -ұялы байланыс операторының желісіне шабуыл
3	Хабарламаларды ұстап қалу	Пакеттерді ұстап қалу	Ұялы байланыс желісіндегі абоненттерге DOS-шабуыл
4	Фрод	Сөйлесулерді жазу	Қызметтік деректерді ұстап қалу

5	Түпнұсқалықты бұзылуы	Байланыс қызметтерін пайдалану үшін абонентпен бүркемелеу	Пайдаланушы деректерін ұстап қалу
6	Орналасқан жерді анықтау	Фрод	Базалық станцияны бұзу
7		Орналасқан жерді анықтау	Коммутациялық және маршруттаушы жабдықтарды бұзу
8			Фрод

2G желісінде негізгі қауіп-қатерлер негізінен пайдаланушы құрылғыларына бағытталған, сондықтан жиі қауіп-қатерлер ұстап қалу және сөйлесулерді жазу, орналасқан жерін және т. б. анықтау болды.

3G желісі деректерді пакеттік тарату базасында толық жұмыс істеді, сондықтан шабуылдар алдыңғы буыннан ерекшеленеді. Пакеттерді ұстап қалу арқылы дауысты тыңдау, орынды анықтау мүмкіндігі пайда болады. Сондай-ақ зиянкестер жалған базалық станцияны пайдалана отырып, сөйлесулерді жазу немесе ұстап қалу, деректер пакеттерін оқу жүзеге асырылады.

4G желісінде жылдамдық, пайдаланушылар мен функционал айтарлықтай өсті. IP/Ethernet базасында толық жұмыс істей бастады. Сондықтан шабуылдар спектрі артады. Жоғары жылдамдықтардың арқасында пайдаланушы мәліметтері ғана емес, ядро желісі де қауіп төндіреді. Коммутаторды немесе маршрутизаторды бұзудың салдары үлкен мәселелерге әкеліп соғады.

1.3 5G мобильді желілеріндегі негізгі қауіпсіздік мәселелері

5G жалпы қоғамдық қызметті қорғауды қамтамасыз ету үшін үлкен қауіпсіздікті талап ететін аса маңызды инфрақұрылымды біріктіреді. Мысалы, онлайн электрмен қоректендіру жүйелерін бұзу адамдардың өміріне әсер ететін барлық электр және электрондық жүйелерде апатты әсер етуі мүмкін. 5G желісіндегі көптеген деректер үлкен рөл атқарады, бұл деректер зақымдалған кезде мәселелер ауқымды болуы мүмкін. Сондықтан қауіпсіздік мәселелерін зерттеу және анықтау және желінің барлық учаскелерінде қауіпсіздікті қамтамасыз ету үшін шешімдерді қарастыру өте маңызды. 5 желісіндегі негізгі мәселелер [13]:

- Радио интерфейс шабуылдары. Абонент пен базалық станция арасындағы сымсыз арнаға шабуылдар;
- Деректердің тұтастығына шабуылдар. Желідегі деректер тұтастығының бұзылуына бағытталған шабуылдар;
- Есептік деректерге шабуыл. Ұялы байланыста пайдаланушылардың есептік деректерін бұзуға бағытталған шабуылдар;

- Роумингке шабуыл. Роумингті бір оператор желісінен басқа мобильді оператор желісіне жаңарту болмаған жағдайда. Осыған байланысты роуминг қауіп төндіруі мүмкін және оны қаскүнемден бұзу ықтималдығы бар;

- DOS-шабуыл деп аталатын жүйені істен шығаруға бағытталған шабуылдар. Соңғы уақытта ең жиі кездесетін DDOS-шабуылдар болып табылады және олар байланыс арналарының пакеттерімен толтыруға бағытталған, бұл олардың істен шығуына әкеледі;

- Пайдаланушыларға бағытталған DOS-шабуылдар. 5G желісінде пайдаланушы құрылғыларын істен шыққанға дейін жеткізеді. Бағдарламалық жасақтаманы бұзуға қабілетті.

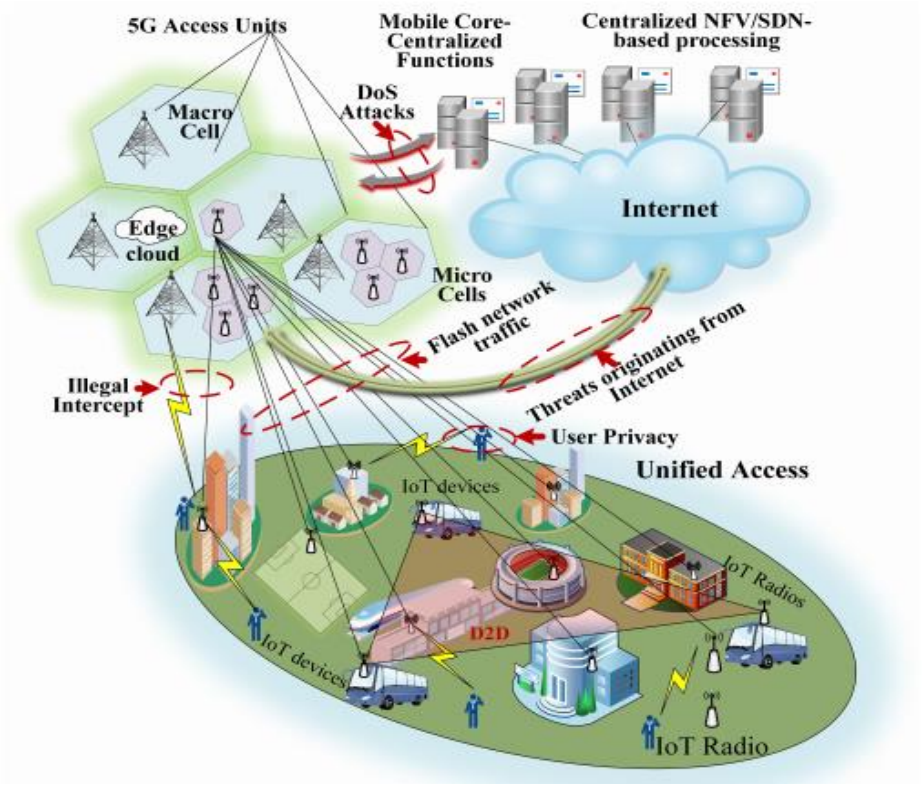
3GPP жұмыс тобы қауіпсіздік пен құпиялылық талаптарын анықтауға, сонымен қатар 5G архитектурасы мен қауіпсіздік хаттамаларын анықтауға белсенді қатысады [14]. Open Networking Foundation (ONF) SDN және NFV қабылдауды тездетуге арналған және техникалық қауіпсіздік сипаттамаларын қоса, техникалық сипаттамаларды жариялайды [15].

NGMN-де көрсетілген 5G жобалау қағидаттары: ортақ композитті ядро құру және жаңа есептеу және желілік технологияларды қолдану арқылы операциялар мен басқаруды жеңілдету. Сондықтан, NGMN-да негізделген, яғни ұялы бұлт, SDN және NFV жобалау қағидаларына сәйкес келетін технологиялардың қауіпсіздігіне және осы технологиялар немесе олардың арасында қолданылатын байланыс желілерінің қауіпсіздігіне назар аударды қ. Пайдаланушылардың жеке өміріне қатысты алаңдаушылықтың артуына байланысты ықтимал құпиялылық мәселелері де назардан тыс қалмады. Шабуылдардың негізгі түрлері 3-кестеде келтірілген, сонымен қатар мобильді желіге шабуылдардың мақсатты нүктелері сипатталған.

1.3 кесте - 5G ұялы байланыс желісіндегі шабуылдардың негізгі түрлері [13]

Шабуыл түрі	Мақсатты нүкте
DOS-шабуыл	Ядро және желіні басқару деңгейі
Сигнал дауылдары	5G желі элементтері
Конфигурацияға бағытталған шабуылдар	Коммутаторлар, маршрутизаторлар
Пайдаланушылық және есептік деректерге шабуылдар	Пайдаланушылардың деректер қоры
TCP деңгейіндегі шабуылдар	SDN контроллеріне шабуыл
«Ортадағы адам» шабуылы	SDN контроллері
IP-спуфинг	Басқару арналары
Сканерлеуші шабуыл	Радио интерфейстер
Қауіпсіздік кілттеріне шабуылдар	Шифрланбаған арналар

Уақыт бойынша шабуылдар	Абоненттің орналасқан жерін бұзу
Шекаралық шабуылдар	Абоненттің орналасқан жерін бұзу
IMSI аулау	Пайдаланушы құрылғысына немесе SIM картасына шабуылдар



1.9 сурет - 5G желісі және ықтимал қауіптер ландшафты

1.4 Мобильді желіде бұлтты сервистердің қауіпсіздігі мәселелері

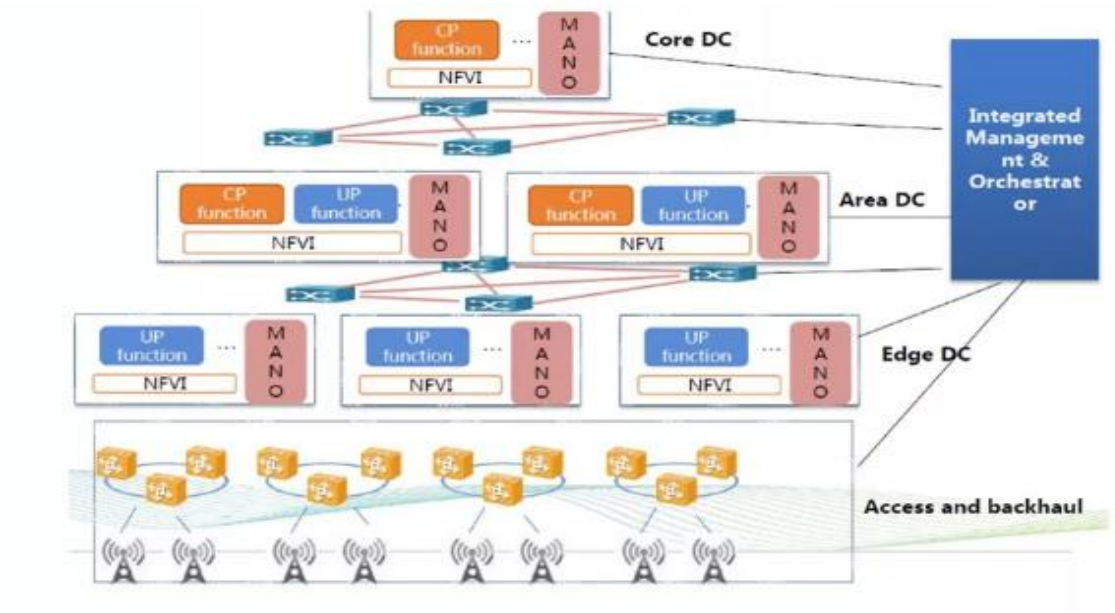
Бесінші буын желісінде бұлт технологиясы үлкен даму қарқынына ие болады. Бұлттық есептеу жүйелері пайдаланушылар бірлесіп пайдаланатын әр түрлі ресурстарды қамтиды. Соңғысы зиянды трафикті таратуы мүмкін, бұлт бүкіл жүйенің технологиясын төмендетеді, көбірек ресурстарды пайдаланады немесе басқа пайдаланушылардың ресурстарына құпия түрде қол жеткізеді. Мобильді бұлтты есептеу (МБЕ) 5G жүйелеріне бұлтты есептеу туралы түсінік береді. Бұл негізінен 5G-дегі архитектуралық және инфрақұрылымдық модификациядан туындайтын мәліметтердің қауіпсіздігінің бірқатар осал тұстарын ұсынады. МБЕ ашық архитектурасы және мобильді терминалдардың әмбебаптығы осалдық тудырады, осылайша шабуылдаушылар мобильді бұлттарда қауіп тудыруы және құпиялықты бұзуы мүмкін [6]. Бұл жұмыста МБЕ қауіптері ұялы құрылғылардың сыртқы, ішкі және желілік қауіпсіздігіне арналған мақсатты бұлт сегменттеріне сәйкес жіктеледі. Сыртқы интерфейс үшін қауіптер қолданба деңгейінде де физикалық деңгейінде де болуы мүмкін, мұнда шабуылдаушылар қолданушы қосымшаларын бұзу немесе құпия ақпарат жинау үшін тыңшылық бағдарламалық жасақтаманы пайдаланады [7]. Ішкі платформа бұлтты серверлерден, деректерді сақтау жүйелерінен, виртуалды

машиналардан және бұлтты қызметтерді көрсету үшін қажет хаттамалардан тұрады. Бұл платформада қауіпсіздікке төнетін қауіп негізінен мобильді бұлт серверлеріне бағытталған. Бұл қауіптердің ауқымы деректерді репликациялаудан HTTP шабуылдарына және XML DoS (HX-DoS) -ге дейін өзгеруі мүмкін [8]. Ұялы құрылғылардың желілік қауіпсіздікке төнетін қауіптері мобильді құрылғыларды бұлтқа қосатын радиоға қол жеткізу технологияларына (RAT) бағытталған. Бұл дәстүрлі Wi-Fi, 4G Long Term Evolution (LTE) немесе 5G-мен бірге келетін басқа жаңа RAT болуы мүмкін. Пайдаланушы құрылғыларға Wi-Fi ұрлау, DoS шабуылдары, мекен-жайларды елемеу және сессияны ұрлау арқылы шабуыл жасауға болады [7]. Бұлт радиосына қол жеткізу желісі (C-RAN) - 5G мобильді бұлттағы қауіпсіздік мәселелерін талдауда маңызды қызығушылық тудырады.

1.5 SDN және NFV қауіпсіздік мәселелері

SDN желіні басқару платформасын орталықтандырады және ұялы байланыс желілерінде бағдарламалау мүмкіндігін қамтамасыз етеді. Алайда, бұл функциялар ұялы желіні бұзуға мүмкіндік береді. Мысалы, орталықтандырылған басқару DoS-шабуылдар үшін қолайлы таңдау болады, ал қолданбалы бағдарламалаудың аса маңызды интерфейстерінің осалдығы (API) бүкіл желінің бұзылуына алып келуі мүмкін [16]. SDN контроллері деректер жолындағы ағын ережелерін өзгертеді, сондықтан контроллердің трафигін оңай анықтауға болады. Бұл контроллерді желіде көрінетін нысанға айналдырады және оны DoS шабуылдарының негізгі мақсатына айналдырады.

NFV болашақ байланыс желілері үшін өте маңызды екендігіне қарамастан, ұялы байланыс жүйелерінің құпиялылығы, тұтастығы және түпнұсқалығы сияқты қауіпсіздіктің негізгі проблемаларына тап болады [15]. Қолданыстағы NFV платформалары виртуализацияланған телекоммуникациялық қызметтер үшін тиісті қауіпсіздік пен оқшаулауды қамтамасыз етпейді [17]. Ұялы желілерде NFV қолдану кезінде туындайтын негізгі проблемалардың бірі - виртуалды желілердің (VNF) функцияларының динамикалық сипаты, бұл конфигурация қателіктеріне демек, қауіпсіздік бұзылуларына әкеледі [19]. Шұғыл назар аударуды қажет ететін негізгі мәселе - гипервизор сынған жағдайда бүкіл желі шабуылға ұшырауы мүмкін [16].



1.10 сурет - 5G ұялы желілерінде SDN және NFV қолдану

1.6 Байланыс арналарындағы қауіпсіздік мәселелері

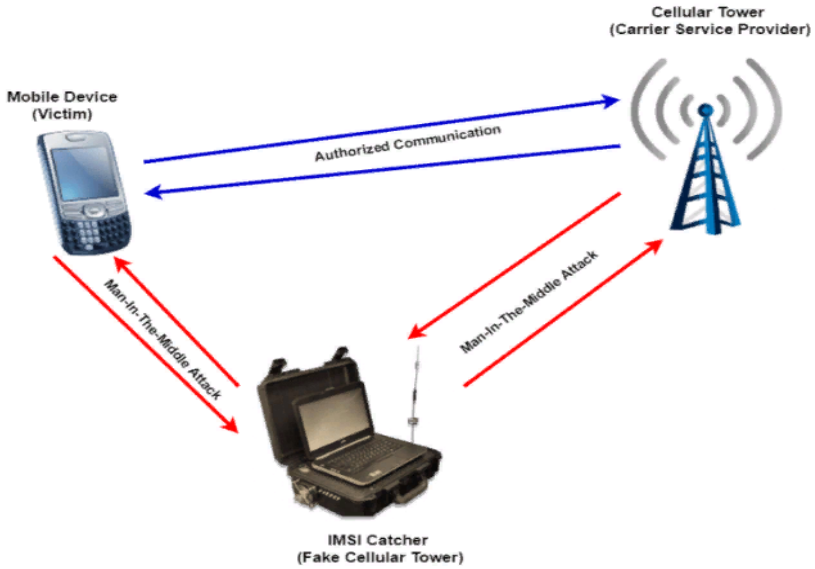
5G ұшқұшсыз басқару құралдары мен әуе қозғалысын басқаруды, бұлтқа негізделген виртуалды шындықты, қосылған көліктерді, ақылды зауыттарды, бұлтты басқаратын роботтарды, көлік пен электронды денсаулық сақтауды қоса алғанда, күрделі экожүйеге ие болады. Осылайша, қолданбаларға жиі аутентификациямен қорғалған және құпиялылықтың көп үлесі бар деректермен алмасуды қолдайтын байланыс жүйелері қажет. Мемлекеттік қызметтерді жеткізушілер, мобильді желі операторлары және бұлтты операторлар осы қызметтерге қосылатын болады. Мұндай экожүйеде Интернетке қол жеткізу деңгейінде де, қызмет көрсету деңгейінде де, қатысушылар арасында жиі аутентификация талап етіледі. Тек ұялы желілерде пайдаланылатын X2, S1, S6, S7 сияқты байланыс интерфейстері осы интерфейстерге шабуыл жасау үшін айтарлықтай білім деңгейін талап етеді. Алайда, SDN негізінде 5G желілері мұндай бөлінген интерфейстерге ие болмайды, ал SDN жалпы интерфейстері болады. Бұл интерфейстердің ашықтығы зиянкестер тарапынан шабуылдардың мүмкіндігін арттырады. 5G ұялы желілеріндегі байланыс SDN негізінде үш байланыс арнасына бөлінуі мүмкін: деректер арнасы, басқару арнасы және бақылауаралық арна [17]. Қазіргі SDN жүйесінде бұл арналар TLS (Transport Layer Security) / SSL (Secure Sockets Layer) сеанстарының көмегімен қорғалған. Бірақ TLS / SSL сеанстары IP деңгейіндегі шабуылдар үшін өте осал, SDN сканерлеріне шабуылдар [23] және аутентификацияның сенімді механизмдері жоқ [18].

1.7 5G желісіндегі құпиялылық мәселесі

Пайдаланушының көзқарасы бойынша негізгі құпиялылық проблемалары пайдаланушылардың мәліметтеріне, орналасқан жеріне және жеке басына шабуыл жасау кезінде пайда болуы мүмкін [25]. Смартфонның көптеген қосымшалары орнатудан бұрын абоненттің жеке деректері туралы егжей-

тегжейлі ақпаратты қажет етеді. Бағдарламаны жасаушылар деректердің қалай сақталатындығы және ол қандай мақсатта қолданылатындығы туралы сирек айтады. Уақыт бойынша шабуылдар мен шекаралық шабуылдар негізінен абоненттердің орналасқан жерінің құпиялылығына бағытталған [19]. Халықаралық абоненттік сәйкестендіргішті (IMSI) қолданатын шабуылдарды IMSI абоненттік пайдаланушы жабдықтарын (UE) ұстап, абонентті анықтау үшін пайдалануға болады. Мұндай шабуылдар, сондай-ақ, UE негізгі базалық станция ретінде қарастыратын жалған базалық станцияны орнатудан туындауы мүмкін, сондықтан абоненттер өздерінің IMSI-ге жауап береді. Сонымен қатар, 5G желілерінде виртуалды ұялы байланыс операторлары (VMNO), байланыс операторлары (CSP) және желілік инфрақұрылым провайдерлері сияқты әртүрлі клиенттер бар. Бұл нысандардың барлығында деректер қауіпсіздігі мен құпиялылықтың әр түрлі басымдықтары бар.

Осы қатысушылар арасындағы сәйкессіздік құпиялылық саясатын синхрондау 5G желісінің қауіпсіздігін құру үшін проблема болып табылады [28]. Алдыңғы буындарда ұялы байланыс операторлары жүйенің барлық компоненттеріне тікелей қол жетімділік пен бақылауға ие болды. 5G ұялы байланыс операторлары жүйені толық басқаруды жоғалтады, өйткені олар CSP сияқты жаңа абоненттерге сенеді. Осылайша, 5G операторлары қауіпсіздік пен құпиялылықты толық бақылауды жоғалтады [29]. Пайдаланушылар мен деректердің құпиялылығы VMNO және басқа да бәсекелестер сияқты әртүрлі субъектілер бірдей инфрақұрылымды бөлісетін ортада елеулі түрде бұзылады. Сонымен қатар, 5G желісінің физикалық шектері жоқ, өйткені олар бұлтты сақтау және NFV мүмкіндіктерін пайдаланады. Демек, 5G операторлары бұлтта деректердің қай жерде сақталатынын тікелей басқара алмайды. Деректерді қорғау тетіктері әр түрлі елдерде олардың артықшылықты контексіне байланысты әр түрлі болғандықтан, пайдаланушының деректері басқа елде бұлтта сақталатындығына қатысты құпиялылыққа күмән келтіріледі [20].



1.11 сурет - Жалған базалық станция арқылы IMSI шабуылының типтік үлгісі

2 5G желісіндегі ақпараттық қауіпсіздікті ұйымдастырудың шешімдері

2.1 5G желісінің қауіпсіздік талаптары

5G PPP құжатына сәйкес қауіпсіздік, деректерді қорғау және құпиялылық деңгейі кем дегенде 4G деңгейіне сәйкес болуы тиіс. Яғни, 5G қол жетімділіктің, ақпарат қауіпсіздігінің, тұрақтылықтың, кідірістің, қол жеткізуді басқарудың барлық деңгейлерінде SLA-ға қолдау көрсете алуы керек [3].

5G ұялы байланыс желілерінің жұмыс істеуі үшін өзара аутентификация, авторизация, деректерді есепке алу және шифрлеу қажет. Сондай-ақ алдынғы хаттамалардағы қауіпсіздік бойынша барлық кемшіліктерді түзету маңызды.

Қауіпсіздік мәселелері OSI моделінің бірнеше деңгейлерінде және әртүрлі домендерде шешілуі тиіс. Сондықтан қауіпсіздік процестерін автоматтандыру да маңызды, ол динамикалық бейімделуге тиіс.

Ұялы байланыс желілерінің жаңа буындарының қауіпсіздігі үшін жүйені бақылау, қауіпсіздіктің негізгі қатері, рұқсат етілмеген бұзушылықпен күресу үшін маңызды. Шабуылдардың алдын алу, сондай-ақ ықтимал шабуылдардың алдын алу және олардың туындауына жол бермеу үшін болжау да көмектесе алады. Мониторингті ұйымдастыру үшін талдау және деректер жинау қажет.

Деректерді басқару желінің барлық учаскелерінде толық келісілуі тиіс. Орталықтандырылған өтпелі басқару айтарлықтай артықшылыққа ие.

Бірнеше жаңа буын ұялы байланыс операторларының өзара әрекеттесуінде барлық деңгейлерді операторлар арасында оқшаулауды қолдау керек. Ұялы желінің барлық бөліктері жеке қауіпсіздік құрылымына ие болуы керек.

5G мобильді желісінің қауіпсіздігін VNF сертификатымен жақсартуға болады. Қауіпсіздікті виртуализациялау 5G мобильді желілері үшін басымдық болып табылады [3].

Пайдаланушы мен қызмет трафигін қорғау үшін жүйенің және коммуникациялардың бұзылуын азайту үшін сенімді шифрлауды таңдау қажет. 5-буын желілерін кеңінен енгізу жаңа технологиялармен қатар жүруі керек.

Сонымен қатар, 5G мобильді желілері барлық нормативтік және заңнамалық актілерге толық сәйкес болуы керек.

Қосылыстардың көптігіне байланысты DDOS шабуылдарының алдын алу үшін жағдай жасау керек, бұл бүгінгі күні жүйеге жиі шабуыл болып табылады және жабдықтың істен шығуына немесе байланыс арналарының үлкен жұмысының тоқтап қалуына әкелуі мүмкін.

Пайдаланушы ақпаратының қорғалуы мен құпиялылығын қамтамасыз ету үшін радио интерфейсті жүйеге жасалған шабуылдардан қорғау әлі де маңызды.

2.2 5G желісінің қауіпсіздік шешімдері

Бұл бөлімде 5G ұялы байланыс желісіне арналған ақпараттық қауіпсіздік бойынша шешімдер көрсетіледі. Флэш-желі трафигінің мәселелерін SDN және

NFV қолдану арқылы шешуге болады. SDN және NFV сияқты жаңа технологиялар бұл мәселелерді шығындар тұрғысынан неғұрлым тиімді шеше алады деп саналады. SDN-де контроллер трафик деңгейінің жоғарылағанын көру үшін желілік жабдықтан API арқылы трафиктің өтуі мен қорғалуы туралы статистикалық мәліметтерді жинай алады. NFV көмегімен негізгі бұлттың қызметтері пайдаланушының талаптарын қанағаттандыру үшін перифериряға жіберілуі мүмкін. Сол сияқты, виртуалды желінің фрагменттерін флэш-желілік трафикті басқару үшін тек жоғары тығыздықтағы UE-ге бөлуге болады. Мобильді трафикті қауіпсіз беру үшін деректерді шифрлау және тұтастықты тексеру қажет, ол үшін IPsec хаттамасы қолданылады.

IP security құру кезінде даралы бақылау жүреді және барлық пакеттерді тексеру процедурасы жүреді, бұл ядро маршрутизаторларын DDOS шабуылдарынан қорғайды, өйткені ядро желісі арқылы өткен кезде барлық күдікті пакеттер ескерілмейді. Mac-flood шабуылынан коммутациялық кестені толтыруға болады, бұл инфрақұрылымды бұзып, байланыс үзілуіне немесе тоқтап қалуға әкелуі мүмкін. Сақтану үшін port security функциясы коммутатор порттарында конфигурацияланған. Роуминг қауіпсіздігі барлық пайдаланушылардың әрекеттеріне көрінетін және ұялы байланыс желісіндегі желілік трафиктің параметрлерін білетін орталықтандырылған жүйелердің көмегімен қамтамасыз етілуі мүмкін. Бұл жүйелерге SDN кіреді. Сигналдық дауылдардан қорғауды қамтамасыз ету мобильді станцияның шағын базалық станциялармен тұрақты байланысына және пайдаланушылардың жоғары ұтқырлығына байланысты біршама күрделенген. C-RAN және перифериялық есептеулер бұл мәселелерді шешеді, бірақ NGMN-де көрсетілгендей, осы технологияларды әзірлеу кезінде болашақ желілердің маңызды аспектісі ретінде сигнал трафигінің көбеюін қарастыру қажет [3].

2.1 - кестеде 5G жүйелеріндегі қауіпсіздік шешімдері бойынша қысқаша деректер келтірілген.

2.1 кесте - 5G желісінің қауіпсіздік технологиялары [2]

Қауіпсіздік технологиясы	Негізгі мәні
DOS-табу	Орталықтандырылған бақылау нүктелерінің қауіпсіздігі
Конфигурацияны тексеру	SDN коммутаторларындағы ағын ережелерін тексеру
Кіруді бақылау	SDN және базалық желі элементтеріне қатынауды бақылау
Трафикті оқшаулау	VNF және виртуалды слайстар үшін оқшаулауды қамтамасыз етеді
Арна қауіпсіздігі	Басқару арналары үшін қауіпсіздікті қамтамасыз ету
Жеке тұлғаны тексеру	Роуминг қызметі мен бұлтты сервистер үшін

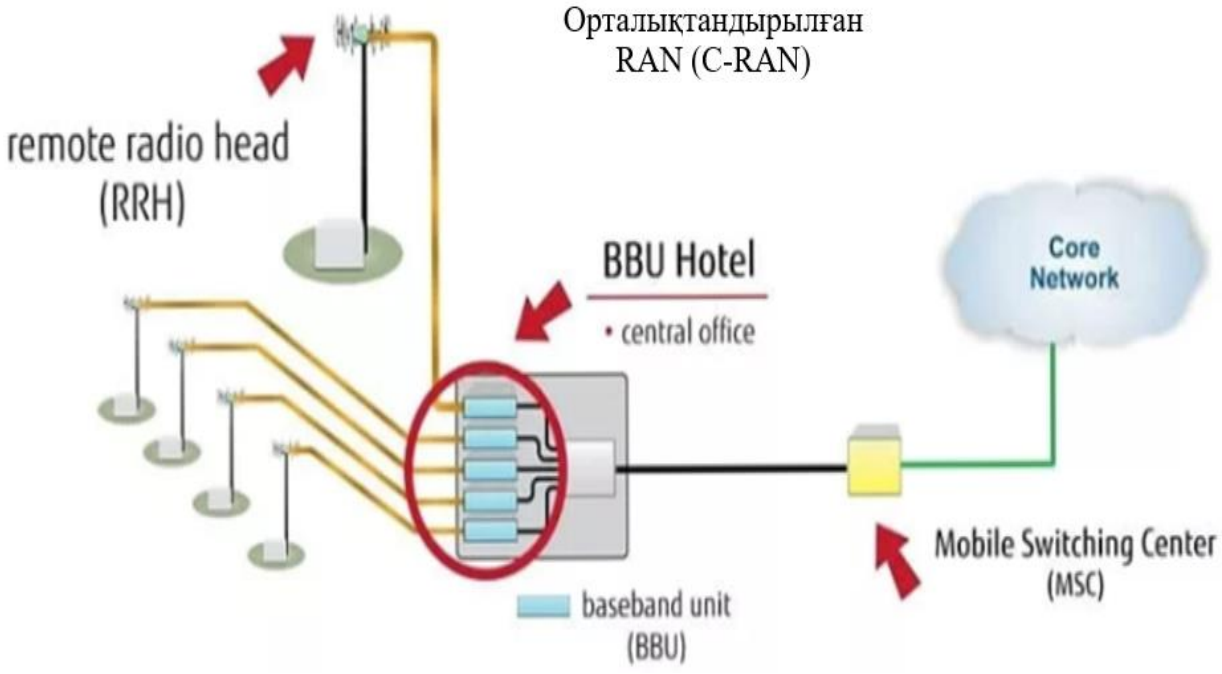
	пайдаланушының жеке басын тексеру
Жеке тұлғаның қауіпсіздігі	Пайдаланушының жеке басының қауіпсіздігін қамтамасыз ету
Орналасу қауіпсіздігі	Пайдаланушының орналасқан жерінің қауіпсіздігін қамтамасыз ету
IMSI қауіпсіздігі	Шифрлау арқылы абонент тұлғасын қорғау
Мобильді терминалдардың қауіпсіздігі	Мобильді терминалдарды қорғау үшін зиянды бағдарламалардан қорғау технологиялары
Бүтіндігін тексеру	Бұлттардағы деректер мен сақтау жүйелерінің қауіпсіздігі
HX-DoS mitigation	Бұлтты веб-сервистердің қауіпсіздігі
Қолжетімділікті сервистік бақылау	Бұлттарға қол жеткізуді сервистік бақылау

2.3 Ұялы желідегі бұлттық сервистердің қауіпсіздік шешімдері

МБЕ-те ұсынылатын қауіпсіздік шараларының көпшілігі виртуалдау технологияларын стратегиялық пайдалану, шифрлау әдістерін қайта жобалау және деректерді өңдеу нүктелерін динамикалық бөлу маңында айналады. Демек, виртуализация бұлт қызметтерін қорғаудың табиғи нұсқасы болып табылады, өйткені әрбір соңғы түйін виртуалды машина (ВМ) арқылы бұлтта нақты виртуалды данаға қосылады. Бұл әр пайдаланушының басқа пайдаланушылардан виртуалды қосылуын оқшаулау есебінен қауіпсіздікті қамтамасыз етеді. Қызметтер негізіндегі шектеу бұлтты есептеу технологияларын қауіпсіз пайдалануға мүмкіндік береді. HX-DoS сияқты қауіпсіздіктің нақты қатерлері үшін нақты шешімдер қолданылады [8]. Мысалы, оқытуға негізделген жүйе пакеттердің белгілі бір санын алады және оларды қауіптерді анықтау және азайту үшін әртүрлі белгілі атрибуттардың мәніне талдайды [9]. Мобильді терминалдарды қауіпсіздендіру үшін, зиянға қарсы бағдарламаларды пайдалану зиянды бағдарламалардың шабуылдарына жалпы тұрақтылықты едәуір арттыруы мүмкін.

Антивирустық шешімдер мобильді терминалда орнатылады немесе бұлттан тікелей орналастырылады және қызмет көрсетіледі [3]. МБЕ деректерін сақтау саласында қауіпсіздік құрылымы деректердің бүтіндігін және сақтау қызметтерін тексеру үшін энергиялық тиімді тетіктерден тұратын болады. Бұл бағдарлама қауіпсіздігі үшін кейбір ұсынылған платформалар бұлттық есептеулер үшін мобильді құрылғыларда икемді қосымшаларды қамтамасыз етуге, пайдаланушылардың идентификаторларын қорғау үшін есептік деректерді генерациялаудың жеңіл динамикалық механизміне, құпиялылықты қорғау үшін кеңістіктік маскалау механизміне, сондай-ақ мобильді есептеулер мен байланыс үшін қауіпсіз бұлтты инфрақұрылымға негізделген MobiCloud [21]. Радиоқатынау желісінің қауіпсіздігі үшін (RAN) бұлтты құрылым ұсынылады, яғни C-RAN, 5G C-RAN бұлттарға арналған RAN желілерін

оңтайландыру және қамтамасыз ету үшін келесі буындағы сымсыз желілерде МБЕ қызметтерінің толассыз өнімділігін динамикалық түрде жақсарта алады. Алайда, бұл қажеттілікті қанағаттандыру үшін C-RAN синхронды цифрлық иерархия (SDH) сияқты дәстүрлі оптикалық желілермен салыстырылатын сенімділіктің жоғары деңгейін қамтамасыз ету қажет және осыған қол жеткізу тәсілдерінің бірі талшықты-сақиналы желі сияқты тетіктерді жаппай енгізу болып табылады.



2.1 сурет - Радиоқолжеткілікті қорғауды қамтамасыз ету үшін CRAN технологиясы

2.4 SDN және NFV үшін қауіпсіздік шешімдері

Ғаламдық желісі бар логикалық орталықтандырылған басқару жазықтығының және бағдарламалау мүмкіндігінің арқасында SDN желілік ресурстардан, күйлерден және ағындардан ақпараттар жинау арқылы қауіптерді жылдам анықтауға мүмкіндік береді. Осылайша, SDN архитектурасы желілік талдауды жеңілдету, қауіпсіздік саясатын өзгерту және қауіпсіздік қызметтерін қосу үшін қауіпсіздіктің жоғары реактивті және проактивті мониторингін, трафикті талдау және жауап беру жүйелерін қолдайды [22]. Ғаламдық желінің көрінуіне байланысты орнықты желінің қауіпсіздік саясатын желі арқылы қолдануға болады, ал брандмауэр және енуді анықтау жүйелері (IDS) сияқты қауіпсіздік жүйелері SDN коммутация кестелерін жаңарту арқылы нақты трафик үшін қолданыла алады. Ұсынылған архитектура көп қолданушы ортадағы виртуалды функциялар үшін ғана емес, сонымен қатар телекоммуникация желісінің физикалық объектілері үшін де қауіпсіздікті қамтамасыз етеді. Жеке ақпаратты аппараттық қорғауды қамтамасыз ету және виртуализацияланған орталарда бүлінген бағдарламалық жасақтаманы анықтау

үшін сенімді есептеулерді, виртуалды жүйелер мен гипервизорлардың тұтастығын қашықтан тексеру мен тексеруді пайдалану мүмкіндігін береді [21].

2.5 5G байланыс арналары үшін қауіпсіздік шешімдері

Желі байланыс каналдарының тиісті қауіпсіздігін тек анықталған қауіптердің алдын алу үшін ғана емес, сонымен қатар SDN-нің қосымша артықшылықтарын, мысалы, орталықтандырылған саясатты басқару, жаһандық желінің күйін және бағдарламалығын қамтамасыз етуді талап етеді. IPsec қазіргі заманғы телекоммуникациялық желілердегі байланыс арналарын қорғау үшін ең жиі қолданылатын қауіпсіздік протоколы болып табылады. 5G байланыс арналарын қорғау үшін IPsec-туннелдеуді пайдалануға болады. Сонымен қатар, ұялы байланыс қауіпсіздігі аутентификация, тұтастық және шифрлеу сияқты әртүрлі қауіпсіздік алгоритмдерін интеграциялау есебінен қамтамасыз етіледі. Пайдаланушымен тікелей байланыс Нір сияқты криптографиялық хаттамалардың көмегімен қорғалуы мүмкін.

2.6 5G желісінде құпиялылықты қамтамасыз ету үшін қауіпсіздік шешімдері

5G құпиялылықты қамтамасыз ету жолдарын іске асыру керек. Ұялы байланыс операторлары өте сезімтал деректерді жергілікті деңгейде сақтай және өңдей алатын және көпшіліктің бұлтында аз сезімтал деректерді сақтай алатын гибридті бұлт әдісі қажет. Осылайша, операторлар деректерге көбірек қол жеткізе алады және оларды бақылай алады, сондай-ақ олардың қай жерде бөлінетінін шеше алады. Осыған ұқсас, 5G-да сервистік-бағытталған құпиялылықты сақтау үшін өміршең шешімге әкеледі [23]. 5G есеп берудің, деректерді барынша азайтудың, ашықтықтың және қолжетімділікті бақылаудың анағұрлым жетілдірілген тетіктері талап етіледі [24]. Демек, 5G стандарттау кезінде қатаң құпиялылық ережелері мен заңдар назарға алынуы тиіс [25]. Реттеуіш тәсілді үш түрге бөлуге болады. Біріншіден, бұл үкімет деңгейіндегі реттеу, онда үкіметтер негізінен нақты елдер үшін және көп ұлтты ұйымдар арқылы құпиялылық ережелерін әзірлейді. Екінші - салалық деңгей, онда 3GPP, ETSI және ONF сияқты әртүрлі салалар мен топтар құпиялылықты қорғау үшін ең жақсы қағидаттар мен әдістерді бірлесіп әзірлейді. Үшіншіден, бұл тұтынушы деңгейіндегі ережелер, онда қалаулы құпиялылық тұтынушылардың талаптарын ескере отырып қамтамасыз етіледі. Орналасқан жердің құпиялылығын қамтамасыз ету үшін, абоненттің нақты тұлғасын жасырып, лақап аттарымен ауыстыра алатын анонимдік әдістерге негізделген әдістер қолданылуы тиіс. Шифрлау тәжірибесі, сондай-ақ, бұл жағдайда пайдалы, мысалы, орналасқан жер (LBS) негізінде қызмет провайдеріне жіберер алдында хабар шифрлануы мүмкін. Орналасқан жер туралы ақпараттың сапасы орналасқан жердің құпиялылығын қорғау үшін төмендегенде, шатастыру сияқты әдістер да пайдалы. Сонымен қатар, орналасқан жерді бүркемелеуге негізделген алгоритмдер уақытша және шекаралық шабуылдар сияқты

орналасқан жердің құпиялылығына кейбір негізгі шабуылдарды өңдеу үшін өте пайдалы [26].

2.7 5G ұялы байланыс ядро желісінің қауіпсіздік шешімі

Құрылған 5G мобильді желісінің жабдықтарына рұқсатсыз кіруден қорғау үшін арнайы AAA сервері қажет. AAA сервері қолданушыларды қосқан кезде үш сатылы процесті: авторизация, аутентификация және есепке алу процестерін өтуге мүмкіндік береді, бұл шабуылдаушылардың қосылуына толықтай жол бермейді. Коммутация кестесінің толып кетуінен қорғау үшін 5G ұялы байланыс операторының желісіне қосылған MAC мекенжайларының санын шектеу керек.

5-ші буынның ұялы желісіндегі магистраль бойымен маршрутизаторлар арасында қауіпсіз беруді ұйымдастыру үшін IPSec-ті IP-ден жоғарылату туралы шешім қабылданды. Сондай-ақ, 5G мобильді желісінің қауіпсіз жолымен мәліметтерді шифрлау және беру алгоритмдерін таңдау қажет. IPSec қолдану, DDOS шабуылдарынан қорғау, 2 маршрутизатордың арасындағы магистральдық желідегі ақпаратты ұстап қалу пайда болады. Осылайша, бағыттауға және мобильді желідегі деректерге шабуылдарды болдырмауға болады.

Коммутация кестесінің толып кетуінен қорғау үшін Cisco қосқыштарындағы Port Security сияқты опцияны пайдалануға болады. Бұл белгілі бір құрылғыларға қол жетімділікті шектеуге, ал басқалары кіруге рұқсат береді. Ұялы желідегі қосылған құрылғылардың санын шектеуге де болады.

5G маршрутизаторлары мен коммутаторлардың шабуылдарынан қорғау үшін AAA-ны қолдануға болады. AAA авторизациялауға, аутентификацияға және оқиғаларды есепке алуға жауапты процестерді білдіреді. Ол үшін Radius және TACACS (TACACS +) хаттамалары қолданылады. Осы екі хаттаманың арқасында пайдаланушының тіркелгі деректерін қорғауға болады және шабуылдаушылар ұялы желідегі жабдыққа қол жеткізе алмайды.

Радиоға қол жеткізу деңгейін қорғау үшін PAP / CHAP хаттамалары қолданылады. Осы екі хаттама қоңырау келіссөздерінің түпнұсқалығын растауға мүмкіндік береді. Аутентификация пайдаланушы құрылғысымен келісе отырып, аты мен паролі бойынша жүзеге асырылады.

2.8 5G ұялы байланыс желісінің магистральдық бөлігінде қауіпсіздікті құру технологиясы

Сенімді және қауіпсіз магистральдық каналды ұйымдастыру үшін біз IPSec технологиясын қолданамыз. Бұл протокол стекі қауіпсіз байланыс арнасы арқылы үлкен трафикті тасымалдауға мүмкіндік береді. Магистральда деректерді беру үшін пакеттерді бір-біріне кедергі жасамай немесе бұзбастан жіберу өте маңызды, өйткені арна немесе сервис арқылы өте маңызды қызметтік немесе пайдаланушының деректері жіберілуі мүмкін. Сондай-ақ DDOS шабуылының жоғары қаупі бар, әсіресе магистральдық жабдық

сегментінде. Берік функционалдығының арқасында IPSec желі қауіпсіздігінің барлық талаптарын толығымен қанағаттандыра алады [27].

IP security - бұл әртүрлі желілік сегменттер арасында IP ақпаратын қауіпсіз таратуға арналған протокол стекі. Бұл стек тұтастықты және аутентификацияны тексере отырып, шифрланған трафикті жіберуге мүмкіндік береді. IPSec хаттамаларының бірі - ғаламдық желідегі қауіпсіз кілттермен алмасу.

Төменгі деңгейлерде қауіпсіз арнаны ұйымдастыру мәліметтерді желі арқылы берудің барлық процестерінің қалай жүретінін көруге мүмкіндік береді, үлкен кемшілігі белгілі бір хаттамаларға міндетті болып табылады.

2.2 сурет - IPsec арнасының типтік үлгісі

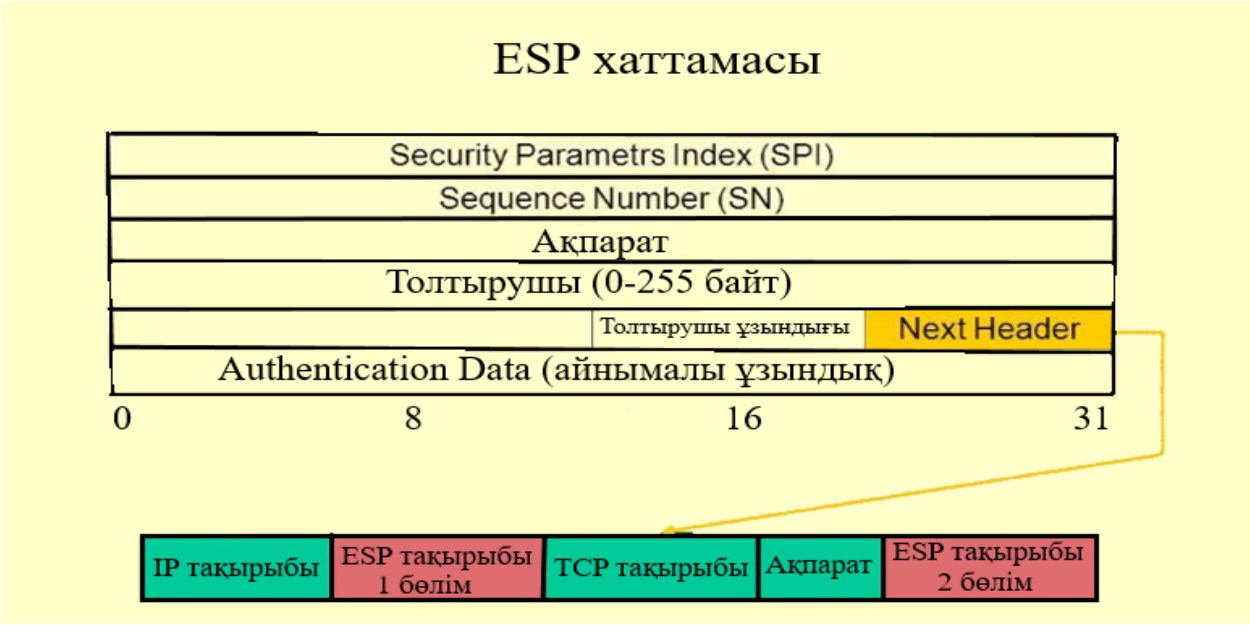
IP security OSI моделінің 3-ші деңгейінде жұмыс істейді және ең танымал протокол - IP қолданады. Сондықтан, протокол бумасы қолдануға ең икемді болып табылады.

IP security негізгі хаттамалары:

- AN протоколы (аутентификация тақырыбы) - байланыс пакеттерінің тағайындалған пунктінің тұтастығы мен аутентификациясы үшін жауап береді және пакеттің қайтадан берілмеуін қамтамасыз етеді;

- ESP протоколы - қауіпсіз арна арқылы берілетін деректерді шифрлауға жауап береді. Сондай-ақ, ол аутентификация тақырыбының кейбір функцияларын орындауға қабілетті;

- ISAKMP протоколы (Интернет қауіпсіздігі қауымдастығы және кілттерді басқару протоколы) IP қауіпсіздігі салынған екі желілік секциялар арасында бастапқы аутентификация мен кілт алмасу үшін жауап береді. Бұл хаттама трафик алмасу үшін жасалған, ол екі желілік сегменттер арасындағы бастапқы қосылу үшін қажет [27].



2.3 сурет - ESP хаттамасының тақырыбы

Security Association - бұл байланыс орнатуды сипаттайтын ұғым. Қауіпсіз байланысты орнату үшін бұл тұжырымдамада деректерді шифрлау әдісі, кэштеу алгоритмі, кілттермен алмасу, әр пакетке белгілі бір нөмір тағайындау қолданылады [1].

Бұл технологияда екі мүмкін жұмыс режимі бар:

- Көлік режимі. Тек желі арқылы жіберілген пакеттің деректері шифрланады. Бұл режим көбінесе бір-бірінен қашықтағы желідегі 2 түйінді қосу үшін қолданылады.

- Туннель режимі. Бұл режимде бүкіл IP пакет шифрланады: тақырыптары, мәліметтері, маршрут туралы барлық ақпарат. Бұл деректер жаңа пакетте жинақталады және осы нысанда желі арқылы жіберіледі. Бұл режим тармақталған қосылымдар мен қауіпсіз арна жасау үшін қолданылады. Бұл режим қолайлы, сондықтан бұл режим кейінірек сипатталады [1].

2.4 сурет - IPsec жұмыс режимдері

Деректерді қауіпсіз арна арқылы жіберу үшін Security Association деп аталатын байланыс құру керек. Пакеттерді екі маршрутизатор арасында қауіпсіз арна бойынша алмасу үшін екі жақта да байланыс орнатылуы керек, себебі қосылу бағыты бір бағытта. Пайдаланушы мен қызметтік деректермен алмасу үшін Security Association бір немесе бірнешеуін қолдану мүмкін.

IKE бүкіл IPsec процесін толықтай байланыстырады. Оның жұмыс принципін екі кезеңге бөлуге болады:

- Екі желілік сегменттер арасында қауіпсіз арна құру. Қауіпсіздік кілттері Diffie-Hellman алгоритмін қолдану арқылы да келісіледі;

- IPsec жалпы қауіпсіздік саясатын құру, IPsec үшін жеке кілттер ауыстырылды.

Қосылу процесі екі жағынан да аутентификациямен ұйымдастырылған. Осыдан кейін ақпаратты қауіпсіз беру үшін шифрлау, тұтастықты тексеру және хаттамалар таңдалады. Бұл хаттамаларға AH және ESP жатады.

Пайдаланушы трафигін беру үшін шифрлау және кэштеу алгоритмдері таңдалуда. Таңдалғаннан кейін пайдаланушы деректерін жіберуге болады.

Шифрлау алгоритмдері ретінде 3DES, ал кэштау - MDA5 таңдаған дұрыс.

Барлық қауіпсіздік қауымдастықтары SAD деректер базасында сақталады. Қауіпсіздіктің бір ассоциациясы келесі SPI элементтерін, алушының IP мекенжайын және ақпараттық қауіпсіздік протоколының идентификаторын қамтиды. Қауіпсіздік протоколының идентификаторына ESP және AH кіреді.

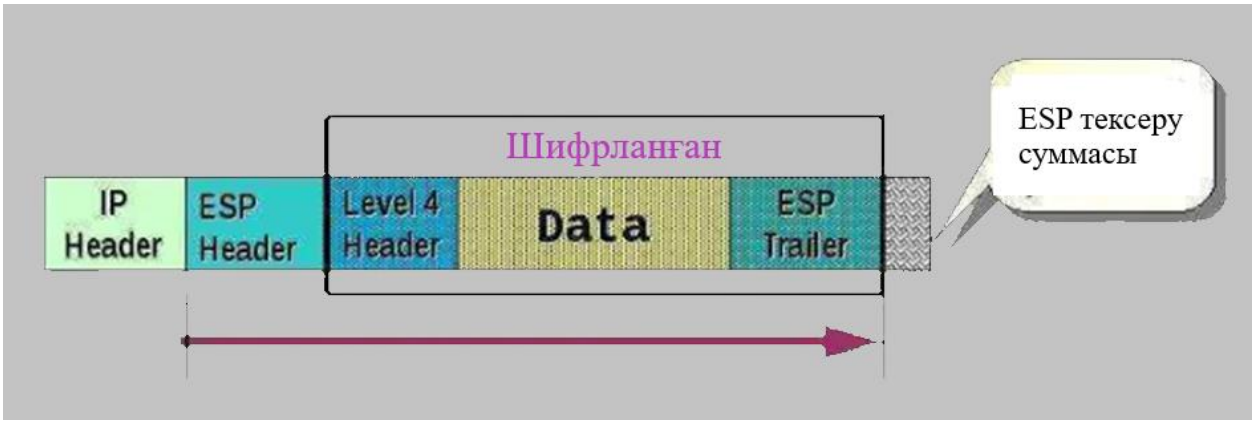
SAD-де шифрлау алгоритмдері, аутентификация және жеке кілттер туралы толық ақпарат бар.

Барлық кіріс пакеттері үшін өңдеу және қолданыстағы қауіпсіздік ережелерімен байланысу үшін маршрутизаторда арнайы SPD дерекқоры бар. Бұл дерекқорда арнайы өрістер алушының IP адресі, бастапқы мекен-жайы, тағайындалған және бастапқы порттары бар.

Орнатылған IP қауіпсіздік арнасы бойынша хабарламаларды жіберу және қабылдау процесін талдаймыз. Пакеттік беру үшін ESP протоколы AN-ге қарағанда артықшылықты бар.

Егер маршрутизатордағы шығатын IPsec пакеттері SA-мен байланысты болса, онда ESP өңдеу басталады. Өңдеу жұмыс режиміне байланысты әр түрлі болады. Туннель режимінде ESP IP-пакетінің тақырыбының инкапсуляциясы жүргізіледі. Содан кейін шифрлау жүзеге асырылады, туннель режимінде пакет бүкіл шифрланған. Шифрлеуден 3DES және AES сияқты алгоритмдерге қолдау көрсетіледі. Шифрланған хабарлама пакеттің пайдалы жүктемесіне орналастырылған. Содан кейін реттік нөмір есептеледі. Басында реттік нөмір нөлге тең болады, жаңа пакеттер келгеннен кейін ол өзгереді, осыған байланысты пакеттерді қайта жіберуді шектеуге болады. Содан кейін ICV тексеру суммасы есептеледі.

Егер кіріс IPsec пакеті маршрутизаторға келіп, ESP тақырыбы мен тіркемесі болса, қабылдайтын IPsec модулі маршрутизаторда тағайындалған IP мекенжайын, ESP, SPI пайдаланып қауіпсіз виртуалды қосылымды іздейді. Егер қауіпсіздік қауымдастығы анықталмаса, пакет өңделмейді және жойылады. Егер SA табылса, сериялық нөмір тексеріледі, сондықтан пакеттерді қайта жіберуден аулақ бола аласыз. Ол үшін жылжымалы терезе әдісі қолданылады. Содан кейін аутентификация процесі жүреді, ол SA-дан үйренеді және ICV мәнімен салыстырылады [27].



2.5 сурет - IPsec-пакетінің типтік үлгісі

Егер келген пакеттің алынған мәні ICV сәйкес келсе, онда пакет жарамды болады,ал керісінше жағдайда жойылады. Бұдан әрі пакет шифрын ашуға беріледі.

Осы барлық қауіпсіздік процедураларының арқасында DDOS-шабуылдардан қорғау деңгейі жоғарылайды,өйткені бүлінген пакеттер жүйемен толығымен жойылады. Магистральды байланыс каналынан өтетін пакеттер ешқандай жолмен шифрленбейді және ұсталмайды.

IPsec жұмыс принципі 5 кезеңнен өтеді:

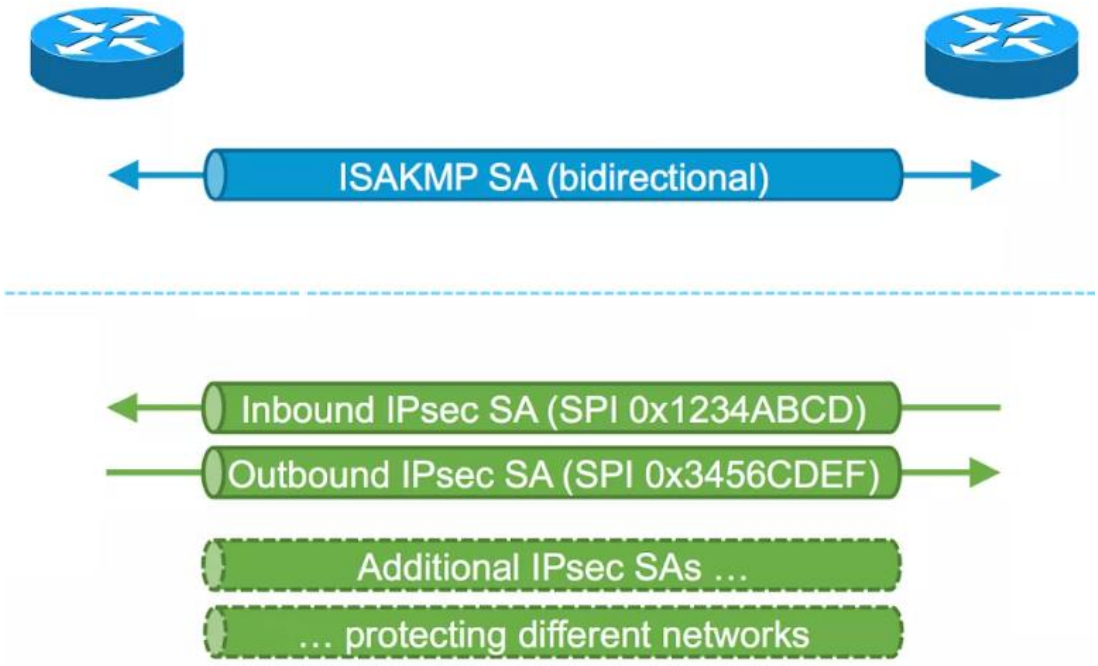
1. Барлық маршрутизаторларда қауіпсіздік саясатын құру, қандай деректер шифрлануы тиіс екенін анықтау;

2. Барлық маршрутизаторларда немесе желіаралық экрандарда қорғалған арнаны ұйымдастыру және екінші фазаға дайындық. Барлық желілік тораптарды аутентификациялау және сәйкестендіру, қорғалған кілттермен алмасу үшін платформаны дайындау және тексеру жүргізіледі. Диффи-Хеллман алгоритмі бойынша барлық L3 құрылғыларда кілттермен алмасу жүреді. Бұл кезеңде қызметтік деректер беріледі;

3. Тікелей қорғалған IPsec арнасын құру. Шын мәнінде, бұл IKE екінші фазасы. IPsec SA барлық параметрлерін келісу, қауіпсіздік қауымдастығын (SA) орнату сияқты функциялар орындалады, сондай-ақ қосымша құпия кілттермен алмасу жүреді.

4. Мобильді желінің қорғалған байланыс арнасы бойынша пайдаланушы мәліметтерімен алмасуды бастау. Бұл кезеңде SA-да орнатылған барлық ережелер қолданылады.

5. IP security қорғалған қауіпсіздік сессиясын аяқтау. Бұл арнаның әрекеті уақыт аяқталған соң немесе осы арнадағы параметрлерді жойғанда тоқтатылады.



2.6 сурет - IPsec жұмыс істеу принципі

2.9 Есептік деректерді қорғауды қамтамасыз ету және AAA рәсімі

Барлық желілік элементтерге және жалпы желіге қатынауды орталықтандырылған және сенімді басқару үшін RADIUS және TACACACS+2 кең таралған хаттамасы қолданылады. RADIUS ХАТТАМАСЫ RFC 2865 құжатында сипатталған. Бұл протоколдар Cisco жабдықтарында сақталады.

AAA механизмі 3 функцияны орындайды: аутентификация, авторландыру және аккаунтинг.

AAA екі түрі қолданылады:

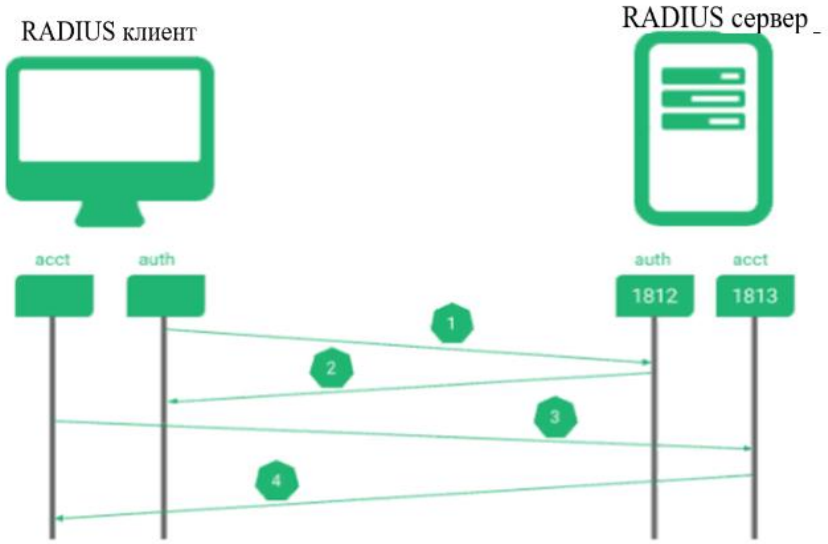
- Желідегі жабдықты әкімшілендіру. Telnet және SSH бойынша жабдықтарды басқару;

- Желіге қатынауды алу үшін барлық есептік деректер мен жабдықтарды сәйкестендіру.

RADIUS хаттамасы авторизациялау, деректерді есепке алу және автоматтандыру үшін IETF-стандартына жатады. RADIUS-клиент-сервер архитектурасы.

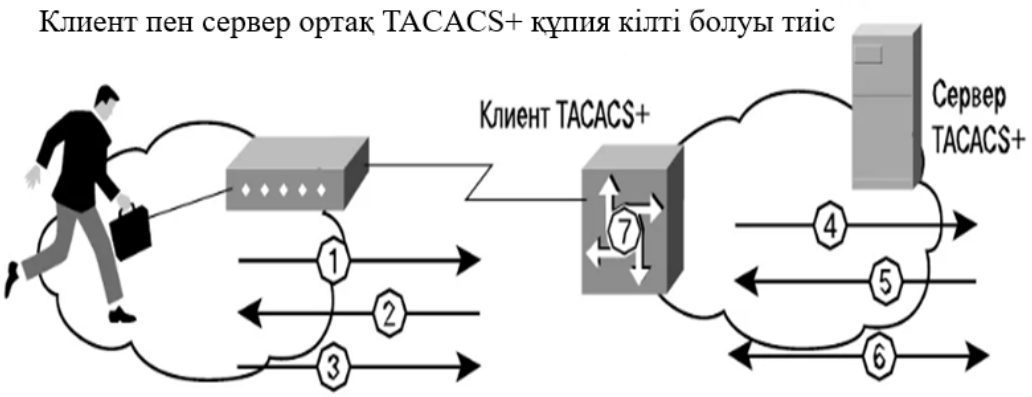
Бұл хаттама аутентификация трафигін NAS-дан AAA-серверге жібереді. Барлық аутентификация және авторизациялау процестері серверге пакеттің бір түрі түседі, ал есепке алу жеке рәсім бойынша жүзеге асырылады. RADIUS протоколы желілік жабдықтың әртүрлі сипатттарымен қолдайды.

RADIUS UDP бойынша жұмыс істейді және аутентификация үшін 1812 порт, ал аккаунтинг үшін – 1813 порт қолданады. Ол Clear text және CHAP сияқты аутентификация түрлерін қолдайды. Шифрлау пароль арқылы жүзеге асырылады [28].



2.7 сурет - RADIUS протоколының жұмыс принципі

TACACACS+ - тек Cisco жабдығымен қолдау көрсетілетін хаттама. Негізгі мақсаты-барлық белсенді желілік жабдықты әкімшілендіру. Сондай-ақ, қорғалатын желіге қолжетімділікті бақылау үшін функционал бар. Бұл хаттама TCP 49 порт бойынша жұмыс істейді. Шифрлау бүкіл пакетте өтеді. Аутентификация, авторизация және деректерді есепке алу жеке функциялармен бөлінген [28].



2.8 сурет - TACACS + протоколының жұмыс істеу принципі

Магистральды жабдыққа қатынауды ұйымдастыру үшін RADIUS-серверді пайдалану ыңғайлы. Жалпы, бұл хаттама тез және желіні өрістету үшін ыңғайлы.

2.10 Коммутаторды коммутация кестесінің шамадан тыс толуынан қорғау

Бүгінгі күні DDOS-шабуылдар әртүрлі масштабтағы таратылған желілер үшін үлкен қауіп төндіреді. Техникалық осындай шабуылдар коммутация кестесін асыра толтыруға бағытталуы мүмкін. Коммутация кестесін асыра толтыру байланыстың жай-күйіне әкеледі, бұл байланыс операторлары үшін өте қажет емес. 5G желісі үшін кез-келген жұмыстың тұрып қалуы байланыс үлкен санынан апатты жағдай болып табылады. Cisco коммутаторларының порттарында Mac-flood-а коммутаторларын қорғау үшін Port security порттарын қорғау технологиясы қолданылады [29].

Port security-коммутациялық жабдықтағы функция. Бұл функция жалпы қосылымдардың санын шектеуге немесе белгілі бір MAC мекен-жайларына кіруге тыйым салуға немесе рұқсат етуге мүмкіндік береді. Осыдан кейін қосылымдар саны командамен шектеледі және одан да көп құрылғылар қосыла алмайды. MAC-адрестерін шектеу кезінде тыйым салынған MAC-адрестерден трафик қабылданбайды.

Бұл функция MAC-адрестердің рұқсатсыз ауысуын болдырмауға мүмкіндік береді және Mac-flood-а-дан толық қорғауға мүмкіндік береді және коммутация кестесінің артық жүктелу қаупінен толық құтылуға болады.

3 Тәжірибелік бөлім

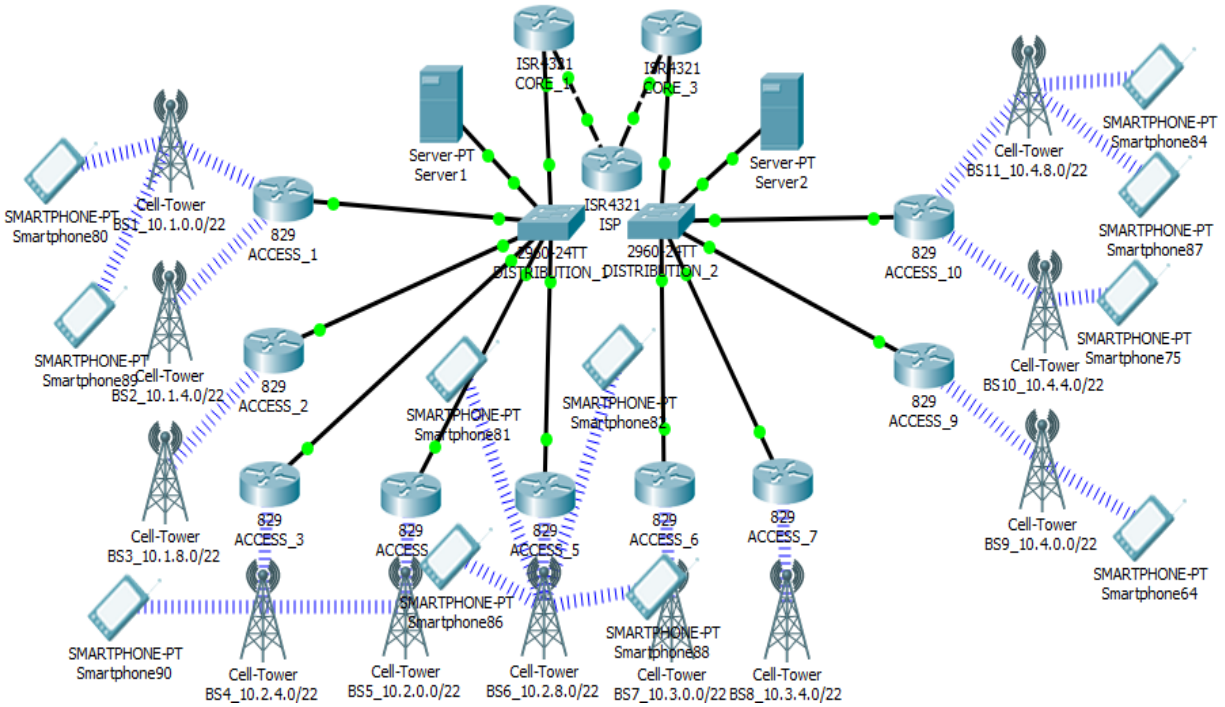
3.1 Cisco Packet Tracer симуляторында жобаланатын 5G желісінің сұлбасы

5 буынды желі сұлбасы 3-деңгейлі архитектурадан тұрады: ядро, тарату, қол жеткізу.

Қол жеткізу деңгейі Cisco 829 маршрутизаторларымен ұсынылған, оған радио интерфейсі бойынша базалық станцияларды қосу ұйымдастырылған.

Тарату деңгейі Cisco 2960 екі коммутаторымен ұсынылған. Оларға қол жеткізу деңгейінің маршрутизаторларын қосу ұйымдастырылады.

Ядро деңгейі IPsec бойынша бір-біріне қосылған 2 маршрутизатордан тұрады.



3.1 сурет - 5G желісінің сұлбасы

3.1 кесте - Жобаланатын желідегі IP-адрестеу және VLAN-дар

Атауы	IP-адрес	VLAN
P2P CORE_1 провайдерімен түйісу	210.210.1.1/30	-
P2P CORE_2 провайдерімен түйісу	210.210.2.1/30	-
1 серверімен P2P	192.168.1.24/30	100
2 серверімен P2P	192.168.2.24/30	200
1 қатынау маршрутизаторы бар P2P	192.168.1.4/30	10
2 қатынау маршрутизаторы бар P2P	192.168.1.8/30	11
3 қатынау маршрутизаторы бар P2P	192.168.1.12/30	12
4 қатынау маршрутизаторы бар P2P	192.168.1.16/30	13
5 қатынау маршрутизаторы бар P2P	192.168.1.20/30	14

6 қатынау маршрутизаторы бар P2P	192.168.2.4/30	21
7 қатынау маршрутизаторы бар P2P	192.168.2.8/30	22
8 қатынау маршрутизаторы бар P2P	192.168.2.16/30	24
9 қатынау маршрутизаторы бар P2P	192.168.2.20./30	25

3.2 IP-адресация мен VLAN-дарды қатынау деңгейіне дейін баптау

Қатынау деңгейі мен желі ядросының маршрутизаторлары арасында P2P интерфейсін баптаудан бастаймыз.

Core_1 маршутизаторында IP-адрестеу параметрлерін баптау мен VLAN-дарды реттеуден бастаймыз:

CORE_1 ядросының маршрутизаторының атауын баптаймыз:

Router(config)#hostname CORE_1

Бірінші серверге дейін интерфейс баптауларын орындаймыз:

CORE_1(config)#interface gigabitEthernet 0/0/1.100

VLAN 100-ды коммутатор жағына GigabitEthernet 0/0/1 интерфейсі арқылы жазамыз**:**

CORE_1(config-subif)#encapsulation dot1Q 100

Кейінен барлық VLAN-дар коммутаторларда қатынау деңгейіне дейін жазылады.

Бұдан кейін желі ядросы мен сервер арасында Point-2-Point IP адресациясын орнату қажет. Біздің жағдайда 3.1 кестеден IP-желі 192.168.1.24 / 30:

CORE_1(config-subif)#ip address 192.168.1.25 255.255.255.252

Деңгейлік маршрутизаторларға интерфейс құру, оларға IP-мекен-жайлар беру және маршрутизаторларға VLAN беру үшін ұқсас параметрлерді орнатамыз.

ACCESS_1 дейінгі маршрутизатордағы параметрлер:

CORE_1(config)#interface gigabitEthernet 0/0/1.10
CORE_1(config-subif)#encapsulation dot1Q 10
CORE_1(config-subif)#ip address 192.168.1.5 255.255.255.252

ACCESS_2 дейінгі маршрутизатордағы параметрлер:
CORE_1(config)#interface gigabitEthernet 0/0/1.11
CORE_1(config-subif)#encapsulation dot1Q 11
CORE_1(config-subif)#ip address 192.168.1.9 255.255.255.252

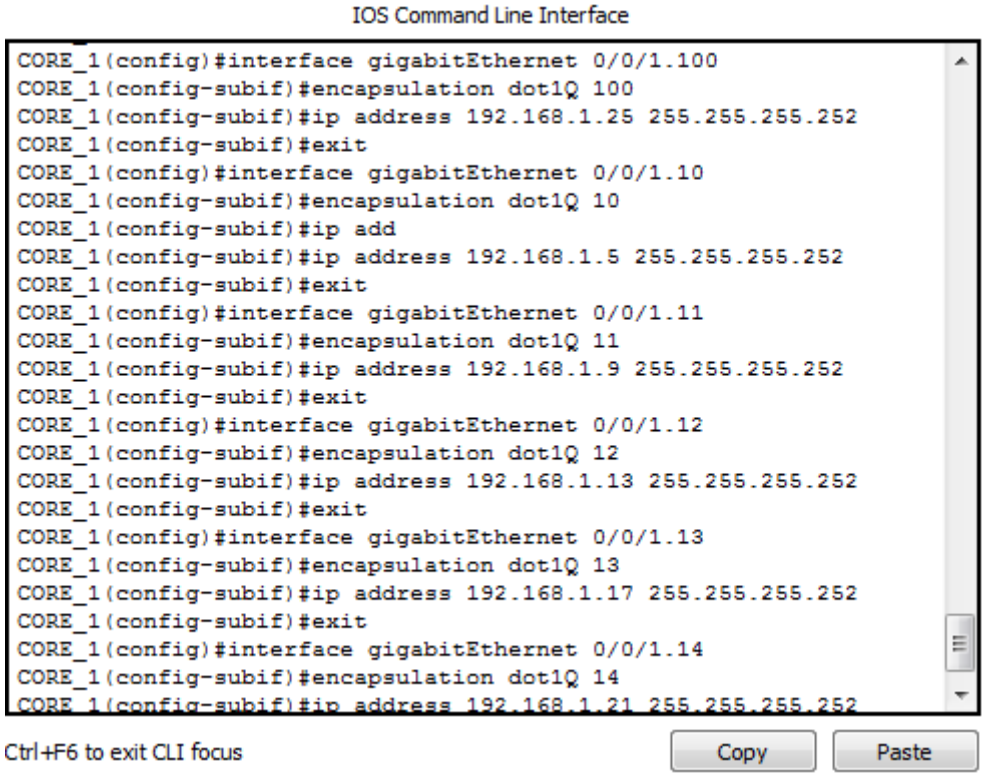
ACCESS_3 дейінгі параметрлер:
CORE_1(config)#interface gigabitEthernet 0/0/1.12
CORE_1(config-subif)#encapsulation dot1Q 12
CORE_1(config-subif)#ip address 192.168.1.13 255.255.255.252

. ACCESS_4 дейінгі параметрлер:

CORE_1(config)#interface gigabitEthernet 0/0/1.13
CORE_1(config-subif)#encapsulation dot1Q 13
CORE_1(config-subif)#ip address 192.168.1.17 255.255.255.252

ACCESS_5 дейінгі параметрлер:

CORE_1(config)#interface gigabitEthernet 0/0/1.14
CORE_1(config-subif)#encapsulation dot1Q 14
CORE_1(config-subif)#ip address 192.168.1.21 255.255.255.252



3.2 сурет - Core_1 маршрутизаторында ішкі интерфейстерді теңшеу

CORE_2 маршрутизаторы бірінші ядро маршрутизаторына ұқсас конфигурацияланған. Параметрлерді CORE_2 маршрутизаторына әкелудің қажеті жоқ, өйткені айырмашылық тек басқа IP мекенжайларда болады, ал барлық параметрлер CORE_2-ге бірдей. Барлық IP адрестер 3.1 кестеде көрсетілген.

Distribution_1 коммутаторында порттардың және VLAN желілерінің конфигурациясы және 5-ші буындағы ұялы байланыс базалық станцияларына жіберу көрсетілген:

Distribution_1(config)#interface FastEthernet0/1

Порт серверге қарай Access режимінде жұмыс істейтінін көрсетеміз:

Distribution_1(config -if)#switchport mode access

Серверге дейінгі VLAN:

Distribution_1(config -if)#switchport access vlan 100

VLAN-ті маршрутизаторлар жағына :ұқсас жазамыз. ACCESS_1 маршрутизаторы жағына VLAN 10 тіркейміз:

Distribution_1(config)#interface FastEthernet0/2
Distribution_1(config -if)#switchport access vlan 10
Distribution_1(config -if)#switchport mode access

ACCESS_2 маршрутизаторы жағына VLAN 11 тіркейміз:

Distribution_1(config)#interface FastEthernet0/3
Distribution_1(config -if)#switchport access vlan 11
Distribution_1(config -if)#switchport mode access

ACCESS_3 маршрутизаторы жағына VLAN 12 тіркейміз:

Distribution_1(config)#interface FastEthernet0/4
Distribution_1(config -if)#switchport access vlan 12
Distribution_1(config -if)#switchport mode access

ACCESS_4 маршрутизаторы жағына VLAN 13 тіркейміз:

Distribution_1(config)#interface FastEthernet0/5
Distribution_1(config -if)#switchport access vlan 13
Distribution_1(config -if)#switchport mode access

ACCESS_5 маршрутизаторы жағына VLAN 14 тіркейміз:

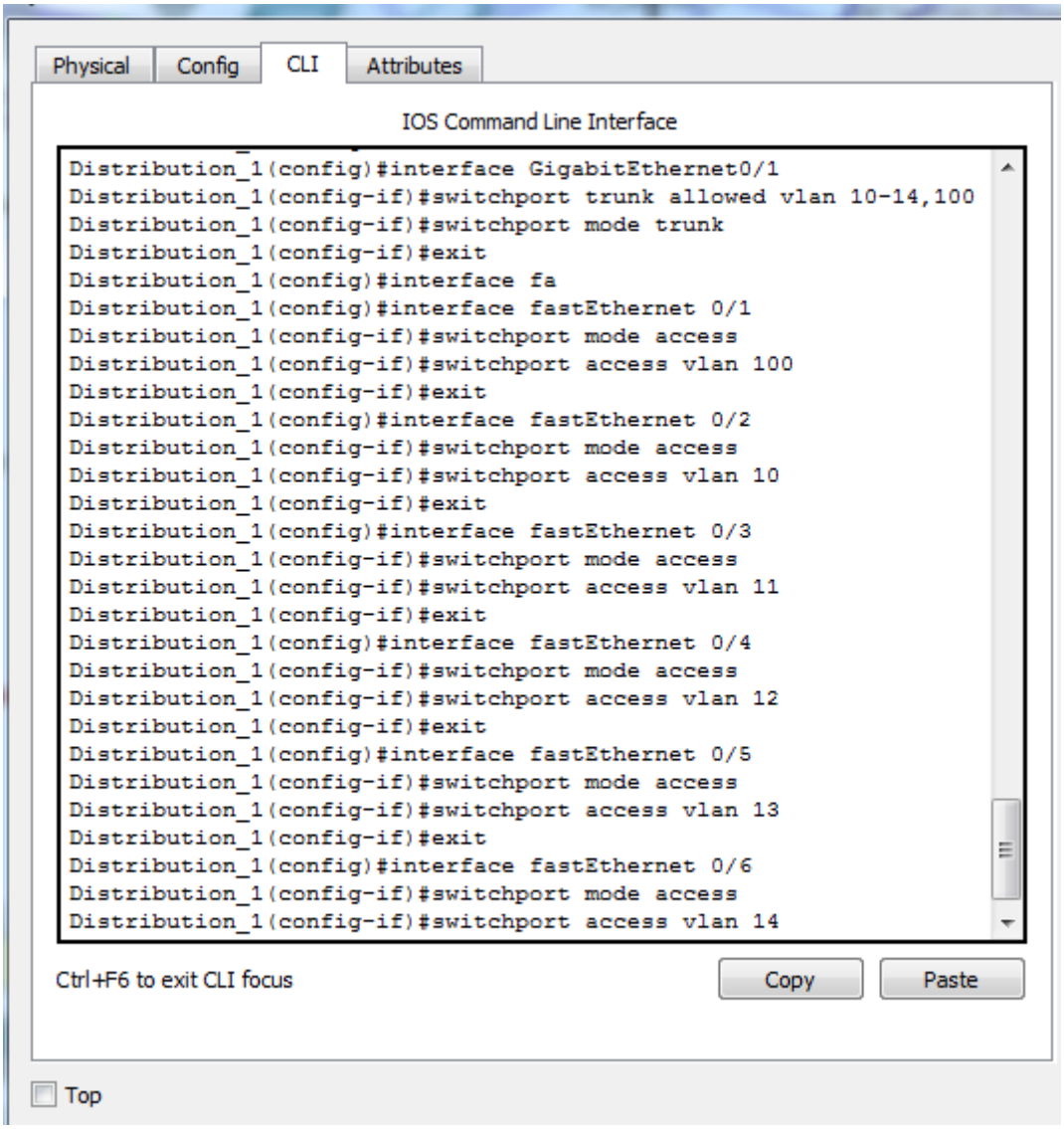
Distribution_1(config)#interface FastEthernet0/6
Distribution_1(config -if)#switchport access vlan 14
Distribution_1(config -if)#switchport mode access

VLAN-ы 10-14 және 100 желі ядросы деңгейінің маршрутизаторы жағына жібереміз:

Distribution_1(config -if)#switchport trunk allowed vlan 10-14,100

Сондай-ақ, ядроға қарайтын порт магистральдық режимде жұмыс істейтінін көрсетеміз:

Distribution_1(config -if)#switchport mode trunk



3.3 сурет - Тарату коммутаторында порттарды теңшеу

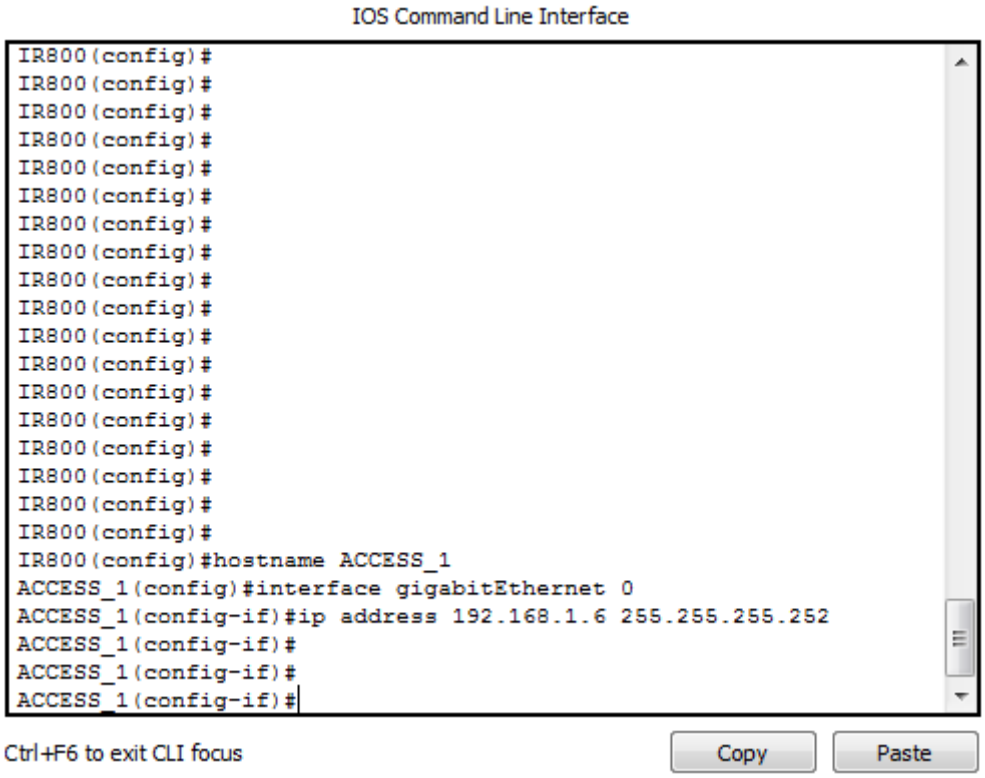
Дәл осындай параметрлер Distribution_2 қосқышында жасалды және Vlan клиенттік құрылғыларда тіркелді, магистральдық порт көтерілді, ал барлық VLANдар магистраль арқылы ядро маршрутизаторына тіркелді.

Барлық маршрутизаторлардағы қол жетімділік деңгейінде интерфейстер тарату қосқыштары бағытында конфигурацияланған және IP мекенжайлары ядро мен кіру маршрутизаторы арасында P2P құру үшін тағайындалады.

ACCESS_1 маршрутизаторындағы параметрлер:

ACCESS_1(config)#interface gigabitEthernet 0

ACCESS_1(config-if)#ip address 192.168.1.6 255.255.255.252



3.4 сурет - Қатынау маршрутизаторында интерфейстерді баптау

Ping командасымен қатынау деңгейінің роутерінен ядро маршрутизаторына қосылуды тексереміз:

```
ACCESS_1#ping 192.168.1.7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.7, timeout is 2
seconds:

Reply to request 0 from 192.168.1.5, 0 ms
Reply to request 1 from 192.168.1.5, 0 ms
Reply to request 2 from 192.168.1.5, 0 ms
Reply to request 3 from 192.168.1.5, 0 ms
Reply to request 4 from 192.168.1.5, 0 ms
```

3.5 сурет – Қосылуды тексеру

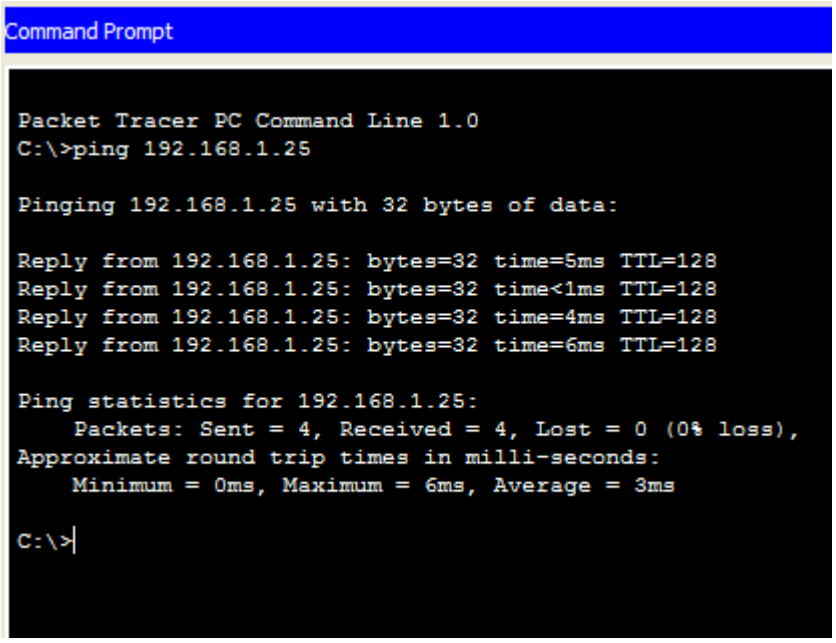
Қосылым бар, бұл барлық параметрлер толығымен дұрыс екенін және қол жеткізу деңгейі мен ядро арасында байланыс бар екенін білдіреді.

Барлық басқа қатынау маршрутизаторларындағы параметрлер ACCESS_1 параметрлеріне толығымен ұқсас болады. Параметрлерде тек әртүрлі IP мекенжайлар болады және олардың барлығы 3.1 кестеде көрсетілген.

3.1-суретте көрсетілген IP мекен-жайы серверде тіркелді.

3.6 сурет - Серверде IP мекен-жайын орнату

Серверден ядро маршрутизаторына ping 3.7 суретте көрсетілген.



3.7 сурет - Серверден ядро маршрутизаторына жүргізілген ping

3.7 суретте біз ping сәтті болғанын көреміз, яғни байланыс бар.

Екінші серверде 192.168.2.24 IP мекенжайы тіркеледі. Екінші жағынан P2P параметрлері толығымен ұқсас. Бірақ барлық қол жетімділік деңгейінің маршрутизаторлары CORE_2 маршрутизаторында және Distribution_2 комутаторына қосылады.

3.3 DHCP және NAT күйге келтіру

Енді әрбір маршрутизатор үшін DHCP-пулды динамикалық режимде абоненттерге беру үшін баптау қажет [1]. Бір базалық станция үшін 1022 мекен-жайдан тұратын жеткілікті пул. Осылайша, бізге 12264 IP-мекенжай қажет.

DHCP хаттамасы қатынау деңгейінің маршрутизаторларында жұмыс істейді және оларға теңшеу қажет.

Ұялы байланыс үшін интерфейсті көтереміз және IP-адресін шлюз ретінде 10.2.0.1 тағайындаймыз, IP-адрестер пулы /22 таңдалды.

Маршрутизаторларда мобильді байланыс құрылғыларын қосу үшін параметрлер орындалады.

ACCESS_4 маршрутизаторынан бастайық:

ACCESS_4(config)#interface cellular 0
ACCESS_4(config-if)#ip address 10.2.0.1 255.255.252.0
Енді маршрутизаторда DHCP көтереміз:

ACCESS_4(config)#ip dhcp pool DHCP

Соңғы мобильді құрылғыларға тарату желісін көрсетеміз. Бұл маршрутизатор үшін 10.2.0/22 желісін таңдаймыз:

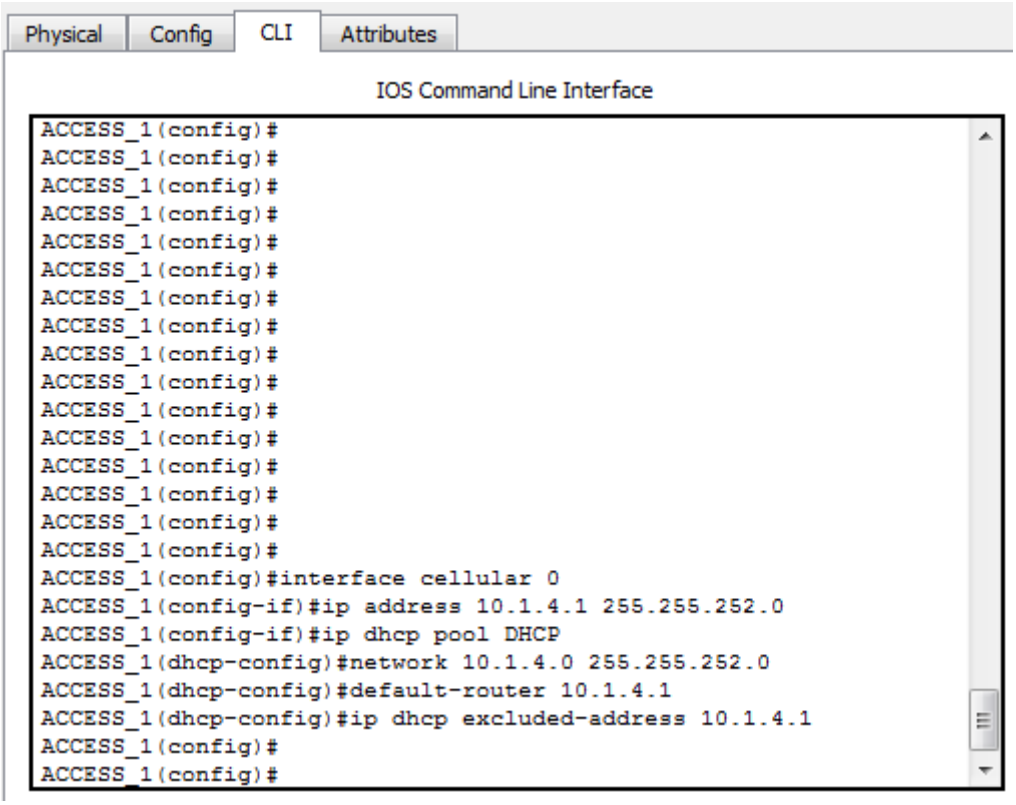
ACCESS_4(dhcp-config)#network 10.2.0.0 255.255.252.0

Шлюз ретінде әдепкі бойынша ACCESS_4 маршрутизаторында шлюздің IP-мекенжайын көрсетеміз:

ACCESS_4(dhcp-config)#default-router 10.2.0.1

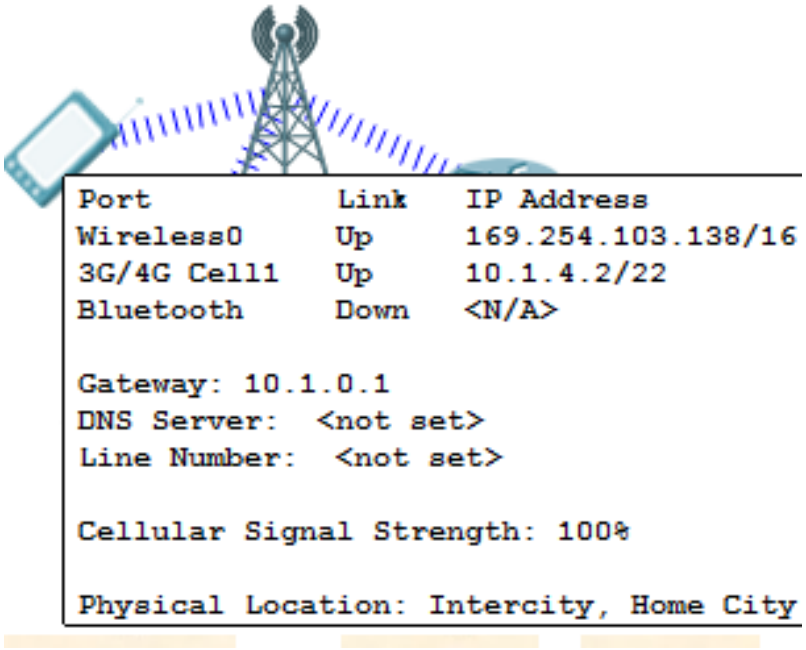
Соңғы пайдаланушыларға берілмеу үшін DHCP шлюзінің мекенжайын беруден шығарамыз:

ACCESS_4(config)#ip dhcp excluded-address 10.2.0.1



3.8 сурет - Желілік интерфейс пен DHCP серверін теңшеу

Басқа маршрутизаторларда параметрлер ұқсас болады. 3.2-кестеде берілген клиенттерге берілетін желілер бойынша мәліметтерді келтірдік.



3.9 сурет - DHCP-шлюзбен IP-адресін алу

3.2 кесте - Клиенттерге берілетін IP-желілер кестесі

Атауы	IP-желі	Шлюздің әдепкі мекенжайы
BS1	10.1.0.0/22	10.1.0.1
BS2	10.1.4.0/22	10.1.4.1
BS3	10.1.8.0/22	10.1.8.1
BS4	10.2.4.0/22	10.2.4.1
BS5	10.2.0.0/22	10.2.0.1
BS6	10.2.8.0/22	10.2.8.1
BS7	10.3.0.0/22	10.3.0.1
BS8	10.3.4.0/22	10.3.4.1
BS9	10.4.0.0/22	10.4.0.1
BS10	10.4.4.0/22	10.4.4.1
BS11	10.4.8.0/22	10.4.8.1

Барлық параметрлерді көрсету қажеттілігі жоқ, себебі басқа маршрутизаторларда баптау толығымен ұқсас. Барлық желілер абоненттерге беріледі және баптау толығымен орындалды.

Енді жаһандық желіге шығу мақсатында ядроның маршрутизаторында NAT технологиясын баптауға өту қажет

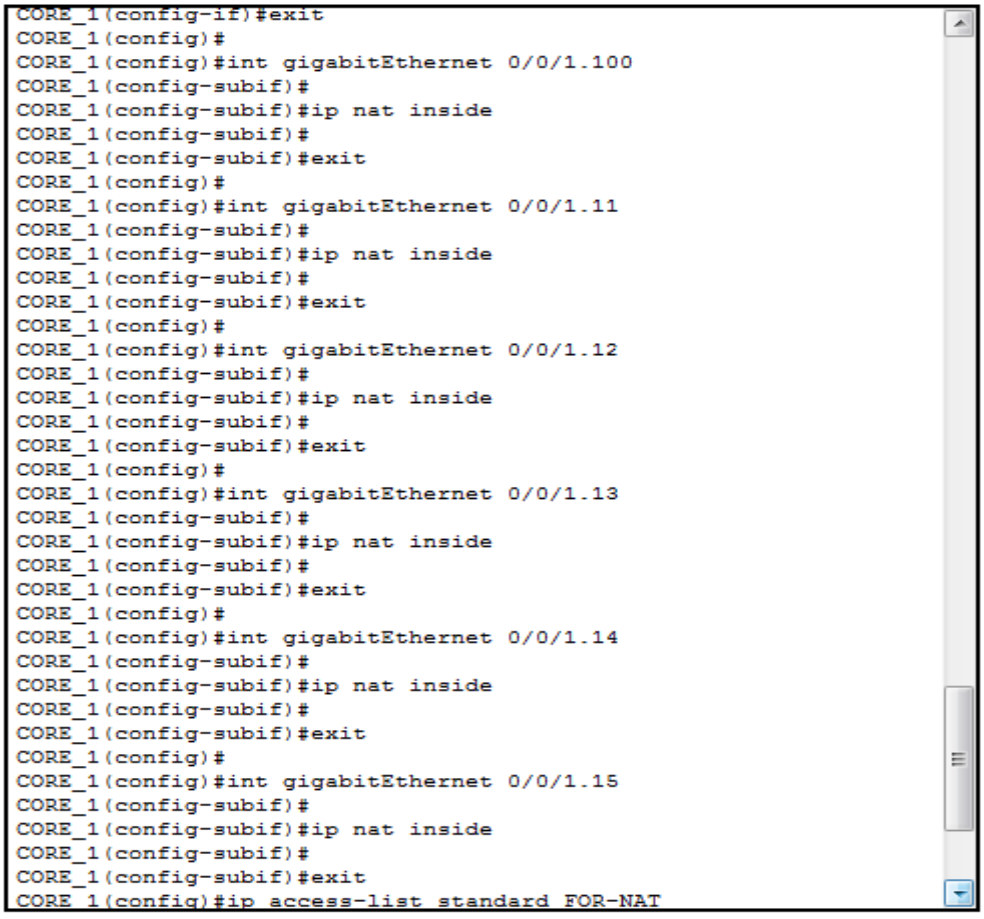
Біздің желіде жеке IP-адрестері қолданылған көптеген қосулар бар. Желіге шығу үшін NAT теңшеу қажет. Осы параметрлерді орындаймыз.

GigabitEthernet 0/0/0 сыртқы интерфейс болады. Барлық мекен-жайлар желіде жария IP арқылы таратылады:

```
CORE_1(config)# interface GigabitEthernet 0/0/0
CORE_1(config-subif)# ip nat outside
CORE_1(config-subif)# exit
```

Енді NAT барлық ішкі интерфейстеріне осы интерфейстердің барлық жеке мекенжайларын сыртқы желіге тарату үшін баптаймыз:

```
CORE_1(config)# int gigabitEthernet 0/0/1.100
CORE_1 (config-subif)#ip nat inside
CORE_1 (config-subif)#exit
CORE_1(config)# int gigabitEthernet 0/0/1.11
CORE_1 (config-subif)#ip nat inside
CORE_1 (config-subif)#exit
CORE_1(config)# int gigabitEthernet 0/0/1.12
CORE_1 (config-subif)#ip nat inside
CORE_1 (config-subif)#exit
CORE_1(config)# int gigabitEthernet 0/0/1.13
CORE_1 (config-subif)#ip nat inside
CORE_1 (config-subif)#exit
CORE_1(config)# int gigabitEthernet 0/0/1.14
CORE_1 (config-subif)#ip nat inside
CORE_1 (config-subif)#exit
CORE_1(config)# int gigabitEthernet 0/0/1.15
CORE_1 (config-subif)#ip nat inside
CORE_1 (config-subif)#exit
```



3.10 сурет - NAT интерфейстерін баптау

Access-list-ті теңшеу және оларға мобильді байланыс желісінің қатынау деңгейі арқылы маршрутизаторға қосылған барлық жеке IP-адрестерді тіркеу қажет:

CORE_1 (config)#ip access-list standard FOR-NAT
CORE_1 (config-std-nacl)#PERMIT 192.168.1.0 0.0.0.255
CORE_1 (config-std-nacl)#PERMIT 10.1.0.0 0.0.255.255
CORE_1 (config-std-nacl)#PERMIT 10.2.0.0 0.0.255.255
CORE_1 (config-std-nacl)#exit

```
CORE_1(config)#ip access-list standard FOR-NAT
CORE_1(config-std-nacl)#PERMIT 192.168.1.0 0.0.0.255
CORE_1(config-std-nacl)#PERMIT 10.1.0.0 0.0.255.255
CORE_1(config-std-nacl)#PERMIT 10.2.0.0 0.0.255.255
CORE_1(config-std-nacl)#exit
CORE_1(config)#ip nat inside source list FOR-NAT interface
gigabitEthernet 0/0/0 overload
```

3.11 сурет - NAT интерфейстерін әрі қарай баптау

Access-list-терді Nat-қа байланыстырамыз және оны интерфейске тіркейкіз:

CORE _1(config)#ip nat inside source list FOR-NAT interface gigabitEthernet 0/0/0 overload

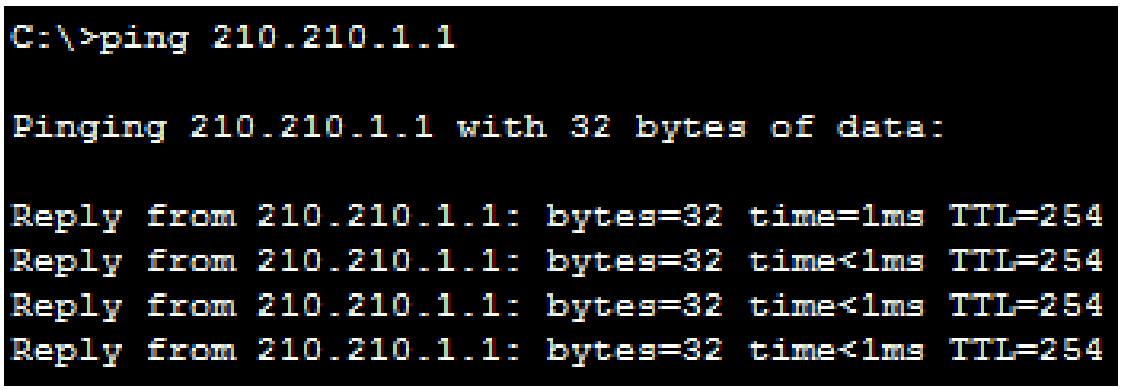
Осындай параметрлер екінші маршрутизаторда орындалды. Ішкі IP мекенжайлары 192.168.2.0/24, 10.3.0.0/16, 10.4.0.0/16. Сыртқы интерфейске 210.2 белгіленген. Провайдер жағына әдепкі бағыт жазылған.

Ping командасы соңғы түйін тарапынан провайдер жағына байланысты тексереміз. Ping бастапқы түпкілікті торабының желісі 10.4.0.0/22-ден маршрутизатордың ядро CORE_2:

```
C:\>ping 210.210.2.1

Pinging 210.210.2.1 with 32 bytes of data:

Reply from 210.210.2.1: bytes=32 time<1ms TTL=254
Reply from 210.210.2.1: bytes=32 time<1ms TTL=254
Reply from 210.210.2.1: bytes=32 time<1ms TTL=254
Reply from 210.210.2.1: bytes=32 time=1ms TTL=254
```

3.12 сурет - 10.4.0/22 желісінен CORE_2 маршрутизаторына Ping

Ping бастапқы түпкілікті торабының желісі 10.4.0.0/22-ден маршрутизатордың ядро CORE_1:



3.13 сурет - 10.4.0/22 желісінен CORE_1 маршрутизаторына Ping

3.4 Ұялы байланыс желісіндегі маршутизация

Ұялы желіде статикалық бағыттауды қолдануға болады [1].

Ядро маршрутизаторларынан қатынас маршрутизаторларына дейінгі статикалық бағыттарды жазамыз.

CORE_1 маршрутизаторында келесі параметрлер орнатылған:

BS4 базалық станцияға желіге кіру үшін тұрақты бағыт ACCESS_3 бағытына қарауы керек:

CORE_1(config)#ip route 10.2.4.0 255.255.252.0 192.168.1.14

BS6 базалық станцияға желіге кіру үшін тұрақты бағыт ACCESS_5 бағытына қарауы керек:

CORE_1(config)#ip route 10.2.8.0 255.255.252.0 192.168.1.18

BS1 және BS2 базалық станцияларына желіге қол жеткізу үшін статикалық бағыт ACCESS_1 бағытына қарауы керек:

CORE_1(config)#ip route 10.1.0.0 255.255.252.0 192.168.1.6
CORE_1(config)#ip route 10.1.4.0 255.255.252.0 192.168.1.6

BS3 базалық станцияға желіге кіру үшін тұрақты бағыт ACCESS_2 бағытына қарауы керек:

CORE_1(config)#ip route 10.1.8.0 255.255.252.0 192.168.1.10

BS5 базалық станциясына желіге кіру үшін тұрақты бағыт ACCESS_4-қа қарауы керек:

CORE_1(config)#ip route 10.2.0.0 255.255.252.0 192.168.1.18

```
CORE_1#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
CORE_1(config)#ip route 10.2.4.0 255.255.252.0 192.168.1.14
CORE_1(config)#
CORE_1(config)#ip route 10.2.8.0 255.255.252.0 192.168.1.18
CORE_1(config)#
CORE_1(config)#ip route 10.1.0.0 255.255.252.0 192.168.1.6
CORE_1(config)#
CORE_1(config)#ip route 10.1.4.0 255.255.252.0 192.168.1.6
CORE_1(config)#
CORE_1(config)#ip route 10.1.8.0 255.255.252.0 192.168.1.10
CORE_1(config)#
CORE_1(config)#ip route 10.2.0.0 255.255.252.0 192.168.1.18
CORE_1(config)#
CORE_1(config)#EXIT
```

3.14 сурет - CORE_1 маршрутизаторында бағыттау

CORE_2 маршрутизаторының жағында дәл осындай параметрлер жасалған. Барлық абоненттік желілерге кіру маршрутизаторлары арқылы қол жеткізуге болады.

CORE_2 маршрутизаторындағы параметрлер:

CORE_2(config)#ip route 10.3.0.0 255.255.252.0 192.168.2.6
CORE_2(config)#ip route 10.3.4.0 255.255.252.0 192.168.2.10
CORE_2(config)#ip route 10.4.0.0 255.255.252.0 192.168.2.18
CORE_2(config)#ip route 10.4.4.0 255.255.252.0 192.168.2.22
CORE_2(config)#ip route 10.4.8.0 255.255.252.0 192.168.2.22

```
CORE_2(config)#ip route 10.3.0.0 255.255.252.0 192.168.2.6
CORE_2(config)#
CORE_2(config)#ip route 10.3.4.0 255.255.252.0 192.168.2.10
CORE_2(config)#
CORE_2(config)#ip route 10.4.0.0 255.255.252.0 192.168.2.18
CORE_2(config)#
CORE_2(config)#ip route 10.4.4.0 255.255.252.0 192.168.2.22
CORE_2(config)#
CORE_2(config)#ip route 10.4.8.0 255.255.252.0 192.168.2.22
```

3.15 сурет - CORE_2 маршрутизаторында бағыттау

Ping командасы әртүрлі бағыттарды байланыстылыққа тексереміз. Core_1 маршрутизаторынан клиенттік құрылғы жағына ping іске қосу:

```
CORE_1#ping 10.1.4.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.4.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
5/10/13 ms
```

3.16 сурет - Core_1 маршрутизаторынан клиенттік құрылғыны тексеру

Команда сәтті орындалды. Енді Core_2 бағытын тексереміз:

```
CORE_2#ping 10.4.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.4.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
10/15/26 ms
```

3.17 сурет - Core_2 маршрутизаторынан клиенттік құрылғыны тексеру

Ping табысты орындалды. Талап еттілген байланыстылық көрсетілді. Ішкі желіні жобалағаннан кейін деректерді қауіпсіздендіру үшін желінің 2 желіні қорғалған арна бойынша қосу қажет.

3.5 IPsec теңшеу және пайдаланушылар мен қызметтік деректерді шифрлау

Енді шифрланған туннельдің тікелей құрылысына өту керек [1].

Басынан бастап бірінші фазаны баптау қажет. Бұл үшін маршрутизаторда ISAKMP саясатын жасаймыз. ISAKMP – бұл интернет ортасында қауіпсіздік қауымдастықтары мен криптографиялық кілттерді орнату үшін RFC 2408-де анықталған хаттама. ISAKMP өзара әрекеттесетін бір жақты торапты аутентификациялау, қауіпсіздік қауымдастықтарын құру және басқару, кілттерді генерациялау және қауіптерді азайту әдістері (мысалы, қызмет көрсетуден бас тарту және қайталанған шабуылдар) үшін рәсімдерді анықтайды.

Бірінші маршутизаторда:

CORE_2 (config)#crypto isakmp policy 100

Сонымен қатар, қызмет көрсету мәліметтерімен алмасу үшін туннель құру үшін қауіпсіздік саясаты алгоритмдерін көрсетеміз.

Шифрлау алгоритмі - 3DES:

CORE_2 (config-isakmp)#encryption 3des

Осылайша, бірінші фазада барлық қызметтік деректер 3DES алгоритмі бойынша шифрланады. Деректер des алгоритмі бойынша 3 рет шифрланады.

Хэштау алгоритмі ретінде таңдалды:

CORE_2 (config-isakmp)#hash md5

Md5 хешлеу алгоритмі VPN арқылы беру кезінде деректердің өзгермейтіндігін бақылауды қамтамасыз етеді.

Кілтті аутентификациялау үшін Pre-shared-key қолданылады:

CORE_2 (config-isakmp)#authentication pre-share

Енді құпия кілттерді алмасу әдісін баптаймыз. Бұл жағдайда Диффи-Хеллман әдісі қолданылады:

CORE_2 (config-isakmp)#group 2

Және, соңғы сессия өмір сүру уақытын белгілеу қажет. Біз 86400 секунд таңдаймыз:

CORE_2 (config-isakmp)#lifetime 86400

Бұдан әрі pre-shared key (аутентификация кілті) теңшеңіз және көршілік мекенжайын көрсетеміз:

CORE_2 (config)#crypto isakmp key med address 210.210.2.2

Құпия кілт ретінде med сөзі таңдалған. Көршісі ретінде 210.210.2.2 адресі белгіленді. Осылайша, 210.210.2.2 дейін туннель салынады. Isakmp сессиясының өмір сүру уақыты 86400 секунд.

Енді 2 фазаны баптаймыз. IPSec теңшеу үшін келесі қадам жасау керек:

- Кеңейтілген ACL құру;
- IPSec Transform құру;
- Криптографиялық карта жасау (Crypto Map);
- Криптографиялық картаны жалпы қол жетімді (public) интерфейске қолдану.

Жоғарыда аталған қадамдардың әрқайсысын қарастырайық.

Одан әрі access-list-та жаңа access-list қосу арқылы қандай трафикті шифрлау керек екенін анықтаймыз:

CORE_2(config)#ip access-list extended FOR-VPN
CORE_2(config-std-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
CORE_2(config-std-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
CORE_2(config-std-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
CORE_2(config-std-nacl)#permit ip 10.1.0.0 0.0.255.255 192.168.2.0 0.0.0.255
CORE_2(config-std-nacl)#permit ip 10.1.0.0 0.0.255.255 10.3.0.0 0.0.255.255
CORE_2(config-std-nacl)#permit ip 10.1.0.0 0.0.255.255 10.4.0.0 0.0.255.255
CORE_2(config-std-nacl)#permit ip 10.2.0.0 0.0.255.255 192.168.2.0 0.0.0.255
CORE_2(config-std-nacl)#permit ip 10.2.0.0 0.0.255.255 10.3.0.0 0.0.255.255
CORE_2(config-std-nacl)#permit ip 10.2.0.0 0.0.255.255 10.3.0.0 0.0.255.255

Сонымен, CORE_1 (Branch_1) аймағында барлық тораптарды қосу үшін бөлінген желілердің әрқайсысынан CORE_2 (Branch_1) аймағында орналасқан желілердің әрқайсысына дейінгі трафик шифрланады.

Деректер қауіпсіздігі үшін қолданылатын түрлендірулер жиынтығын (Transform Set) құрайық. Оны FIRST деп атаймыз:

branch_1(config)#crypto ipsec transform-set FIRST esp-3des esp-md5-hmac

Пайдаланушы деректерін жіберу үшін осы пәрменді пайдалана отырып, біз мыналарды анықтай аламыз:

- ESP - 3DES-шифрлау әдісі;
- MD5-хэштау алгоритмі.

Енді криптографиялық картаны баптауға кірісеміз және барлық аяқталған IPSEC және ISAKMP параметрлерін біріктіреміз [27].

Криптографиялық карта RFT деп аталады:

branch_1(config)#crypto map RFT 100 ipsec-isakmp

Ipsec-isakmp тегі роутерге криптография картасы IPsec картасына жататынын хабарлайды.

Көрші теңқұқұлы адрес ретінде 210.210.2.2 белгілейміз:

branch_1(config-crypto-map)#set peer 210.210.2.2

Бұрын теңшелген FIRST түрлендіру жиынтығы осы ережеге қолданамыз:

branch_1(config-crypto-map)#set transform-set FIRST

Бұл ережеге қажетті трафикті шифрлау үшін бұрын жасалған access-list байланыстырамыз:

branch_1(config-crypto-map)#match address FOR-VPN

Соңғысы бұл ережені 5G маршрутизаторының сыртқы интерфейсіне байланыстыру.

branch_1(config)#interface gigabitEthernet 0/0/0
branch_1(config-if)#crypto map RFT

```
crypto isakmp policy 200
 encr 3des
 hash md5
 authentication pre-share
 group 2
!
crypto isakmp key med address 210.210.2.2
!
!
!
crypto ipsec transform-set FIRST esp-3des esp-md5-hmac
!
crypto map RFT 100 ipsec-isakmp
 set peer 210.210.1.2
 set transform-set FIRST
 match address FOR_NAT
!
```

3.18 сурет - CORE_1 маршрутизаторында IPsec және ISAKMP конфигурациясы

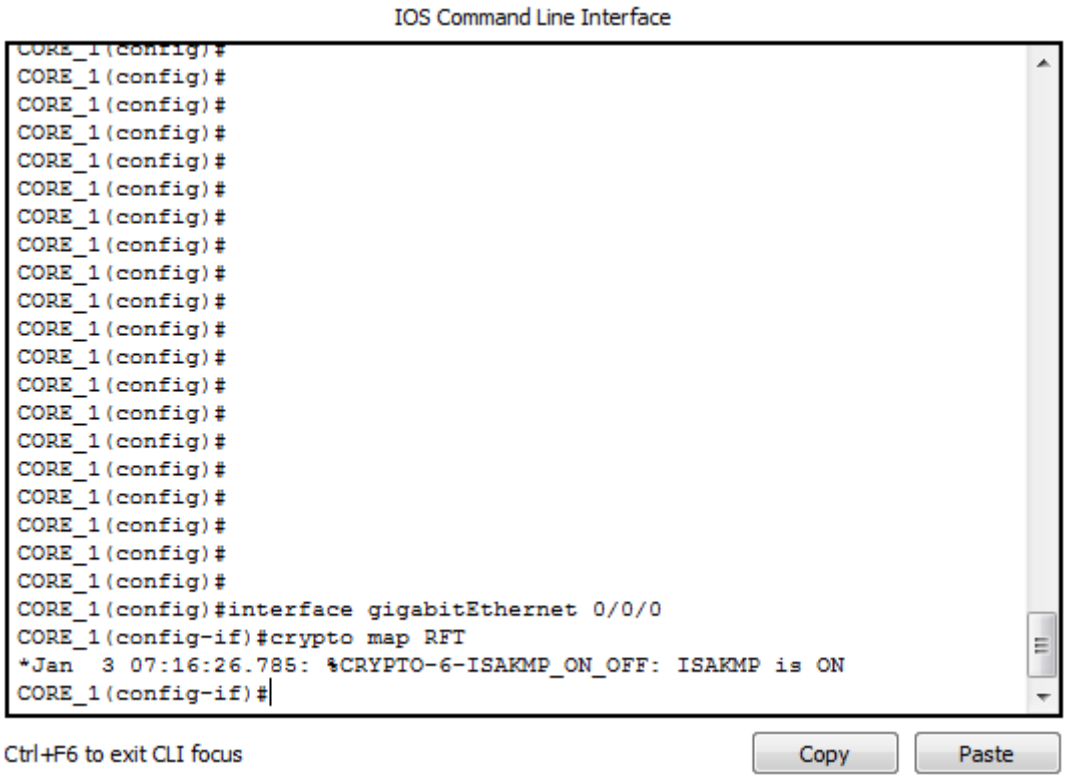
```
ip access-list extended FOR_NAT
 permit ip 10.2.0.0 0.0.255.255 10.3.0.0 0.0.255.255
 permit ip 10.2.0.0 0.0.255.255 192.168.2.0 0.0.0.255
 permit ip 10.2.0.0 0.0.255.255 10.4.0.0 0.0.255.255
 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
 permit ip 192.168.1.0 0.0.0.255 10.3.0.0 0.0.255.255
 permit ip 192.168.1.0 0.0.0.255 10.4.0.0 0.0.255.255
 permit ip 10.1.0.0 0.0.255.255 192.168.2.0 0.0.0.255
 permit ip 10.1.0.0 0.0.255.255 10.3.0.0 0.0.255.255
 permit ip 10.1.0.0 0.0.255.255 10.4.0.0 0.0.255.255
```

3.19 сурет - Желіде шифрланатын трафик

Сонымен, маршрутизаторда осы криптографиялық картаны сыртқы маршрутизатордың интерфейсіне қосыңыз.

CORE_1(config)#interface gigabitEthernet 0/0/0
CORE_1(config-if)#crypto map RFT

Орындалған параметрлерден кейін isakmp криптографиялық саясаты көтерілді және ол белсенді:



3.20 сурет - Криптографиялық картаны сыртқы интерфейске қосу

Ұқсас параметрлер branch_2 маршрутизаторында да орындалды:
crypto isakmp policy 200
encr 3des
hash md5
authentication pre-share
group 2

```
crypto isakmp key med address 210.210.1.2
crypto ipsec transform-set FIRST esp-3des esp-md5-hmac
crypto map RFT 100 ipsec-isakmp
set peer 210.210.1.2
set transform-set FIRST
match address FOR_NAT
ip access-list extended FOR_NAT
permit ip 10.4.0.0 0.0.255.255 10.2.0.0 0.0.255.255
permit ip 10.4.0.0 0.0.255.255 192.168.1.0 0.0.0.255
permit ip 10.4.0.0 0.0.255.255 10.1.0.0 0.0.255.255
permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
permit ip 192.168.2.0 0.0.0.255 10.2.0.0 0.0.255.255
permit ip 192.168.2.0 0.0.0.255 10.1.0.0 0.0.255.255
permit ip 10.3.0.0 0.0.255.255 192.168.1.0 0.0.0.255
permit ip 10.3.0.0 0.0.255.255 10.1.0.0 0.0.255.255
permit ip 10.3.0.0 0.0.255.255 10.2.0.0 0.0.255.255
```

Бұл параметрлер CORE_2 маршрутизаторындағы параметрлерден тек IP мекенжайлары әртүрлі болғандықтан ғана ерекшеленеді, алгоритмдердің барлығы бірдей.

Енді филиалдық маршрутизаторда тоқтатылған 192.168.1.2 мекен-жайы бар түйіннен ping пәрменін пайдаланып, шифрланған желідегі түйіндер арасында Branch.1 маршрутизаторының тоқтатылуында 192.168.2.2 мекен-жайы бар түйінге байланыс бар-жоғын тексерейік:

```
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 210.210.1.1: Destination host unreachable.
Reply from 210.210.1.1: Destination host unreachable.
Reply from 210.210.1.1: Destination host unreachable.
Reply from 210.210.1.1: Destination host unreachable.

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

3.21 сурет - 192.168.1.2 мекен-жайы бар түйіннен 192.168.2.2 мекен-жайы бар түйінге қосылу

ICMP-сұраулар өтпейді және тораптар арасында байланыс жоқ. Ал мәселе сыртқы интерфейсте NAT теңшелген және барлық деректер шифрланбайды және шифрланған VPN-арнасы бойынша берілмейді, ал әдеттегі түрде беріледі.

Маршрутизаторлардың бірінде show ip nat translation командасы барлық сұрау салуларды ping командасы желіге тартылғанын тексере алады, соның есебінен деректер шифрленбейді және қашықтағы жаққа дейін жіберілмейді.

```
branch_1#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 210.210.1.2:30    192.168.1.2:30     192.168.2.2:30     192.168.2.2:30
icmp 210.210.1.2:31    192.168.1.2:31     192.168.2.2:31     192.168.2.2:31
icmp 210.210.1.2:32    192.168.1.2:32     192.168.2.2:32     192.168.2.2:32
icmp 210.210.1.2:33    192.168.1.2:33     192.168.2.2:33     192.168.2.2:33
icmp 210.210.1.2:34    192.168.1.2:34     192.168.2.2:34     192.168.2.2:34
icmp 210.210.1.2:35    192.168.1.2:35     192.168.2.2:35     192.168.2.2:35
icmp 210.210.1.2:36    192.168.1.2:36     192.168.2.2:36     192.168.2.2:36
icmp 210.210.1.2:37    192.168.1.2:37     192.168.2.2:37     192.168.2.2:37
```

3.22 сурет - show ip nat translation командасының нәтижесі

Осылайша, іс жүзінде біз NAT-тің арқасында трафик шифрланған канал арқылы өтпейтініне көз жеткіздік. Access-lista саясатын NAT-қа өзгерту қажет.

Біз стандартты алып тастап, кеңейтілген access list жасадық.

CORE_1 роутерінде біз NAT-ға бағынбайтын және қауіпсіз байланыс каналы арқылы берілмеуі үшін барлық қорғалған трафикке тыйым саламыз, ал қалған трафикке рұқсат етіледі:

ip access-list extended FOR-NAT

Deny дегеніміз, бұл access list трафик тыйым салынады:

deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
deny ip 192.168.0.0 0.0.255.255 10.3.0.0 0.0.255.255
deny ip 192.168.0.0 0.0.255.255 10.4.0.0 0.0.255.255
deny ip 10.1.0.0 0.0.255.255 192.168.2.0 0.0.0.255
deny ip 10.1.0.0 0.0.255.255 10.3.0.0 0.0.255.255
deny ip 10.1.0.0 0.0.255.255 10.4.0.0 0.0.255.255
deny ip 10.2.0.0 0.0.255.255 192.168.2.0 0.0.0.255
deny ip 10.2.0.0 0.0.255.255 10.3.0.0 0.0.255.255
deny ip 10.2.0.0 0.0.255.255 10.4.0.0 0.0.255.255

Permit қалған IP-адрестерден трафик рұқсат етілген дегенді білдіреді:

permit ip 192.168.1.0 0.0.0.255 any
permit ip 10.1.0.0 0.0.255.255 any
permit ip 10.2.0.0 0.0.255.255 any

CORE_2 маршрутизаторында қауіпсіз арнамен шифрлануы және берілуі қажет трафикке тыйым салу керек, ал қалған трафикке 1 негізгі маршрутизатор сияқты рұқсат етіледі:

ip access-list extended FOR-NAT1
deny ip 10.4.0.0 0.0.255.255 10.2.0.0 0.0.255.255
deny ip 10.4.0.0 0.0.255.255 10.1.0.0 0.0.255.255
deny ip 10.4.0.0 0.0.255.255 192.168.1.0 0.0.0.255
deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
deny ip 192.168.2.0 0.0.0.255 10.2.0.0 0.0.255.255
deny ip 192.168.2.0 0.0.0.255 10.1.0.0 0.0.255.255
deny ip 10.3.0.0 0.0.255.255 192.168.1.0 0.0.0.255

deny ip 10.3.0.0 0.0.255.255 10.1.0.0 0.0.255.255
deny ip 10.3.0.0 0.0.255.255 10.2.0.0 0.0.255.255
permit ip 192.168.2.0 0.0.0.255 any
permit ip 10.3.0.0 0.0.255.255 any
permit ip 10.4.0.0 0.0.255.255 any

Қауіпсіз арнаның жұмысын тексереміз. Ол үшін ICMP сұранысын 192.168.2.3 түйінінен 192.168.1.3 түйініне жібереміз:

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=126
Reply from 192.168.1.3: bytes=32 time<1ms TTL=126
Reply from 192.168.1.3: bytes=32 time<1ms TTL=126
Reply from 192.168.1.3: bytes=32 time<1ms TTL=126
```

3.23 сурет - 192.168.2.3 түйінінен 192.168.1.3 түйініне жіберілген ping

Ping командасы арқылы тексеру сәтті өтті. Байланыс бар. ICMP-ді тағы бірнеше рет іске қосыңыз.

Show crypto isakmp sa командасын қолдана отырып, CORE_1 маршрутизаторында сеанстарының 210.210.2.2 және 210.210.1.2 екі түйін арасында ISAKMP орнатылғандығы туралы қорытынды жасауға болады:

```
CORE_1#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot
status
210.210.2.2     210.210.1.2     QM_IDLE           1068    0
ACTIVE
```

3.24 сурет - Show crypto isakmp sa командасының нәтижесі

CORE_2 ISAKMP маршрутизаторында сеанс:

```
Router#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot
status
210.210.1.2     210.210.2.2     QM_IDLE           1049    0
ACTIVE
```

3.25 сурет - CORE_1 маршрутизаторында ISAKMP сессиясын тексеру командасы

Бұл бірінші кезеңдегі конфигурация сәтті өтті және қызмет трафигімен алмасу дегенді білдіреді.

Енді біз show crypto isakmp policy командасын пайдаланып ISAKMP-де қандай параметрлер қабылданғанын тексереміз. Екі маршрутизаторда да шығыс ұқсас. 3des шифрлау ретінде, хэштер - MD5, аутентификация әдісі - Pre-shared key:

```
Global IKE policy
Protection suite of priority 100
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
```

3.26 сурет - CORE_1 маршрутизаторында ISAKMP сессиясын тексеру командасы

Енді екі маршрутизаторда қандай ережелер қолданылатындығын тексеріңіз:

```
CORE_1#sh crypto ipsec sa

interface: GigabitEthernet0/0/0
    Crypto map tag: RFT, local addr 210.210.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
   current_peer 210.210.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 0
   #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 210.210.1.2, remote crypto endpt.:210.210.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0/0
     current outbound spi: 0x60573EF4(1616330484)

     inbound esp sas:
      spi: 0x3A8309FA(981666298)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 2009, flow_id: FPGA:1, crypto map: RFT
    sa timing: remaining key lifetime (k/sec): (4525504/3033)
    IV size: 16 bytes
    replay detection support: N
    Status: ACTIVE
 outbound esp sas:
  spi: 0x71366A83(1899391619)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 2010, flow_id: FPGA:1, crypto map: RFT
    sa timing: remaining key lifetime (k/sec): (4525504/3033)
    IV size: 16 bytes
    replay detection support: N
    Status: ACTIVE
```

3.27 сурет – Маршутизатор ережелері

Қорытындыда командада біз 6 пакеттің шифрланғанын және инкапсуляцияланғанын көріп отырмыз, барлығы CORE_1 маршутизаторында

қайта шифрланған және деинкапсуляцияланған. Жетінші пакеттің қайта шифрленуі қызметтік деректер берілуімен байланысты. Команда осы маршрутизаторда қандай ассоциациялар бар екенін көрсетеді. Біз ESP (кіру және шығу) үшін 2 ережелері бар екенін көреміз. ESP SAS кіріс және шығысында шифрлау алгоритмі – 3des, ал кештеу – md5 қолданылған. Ipsec туннель режимінде жұмыс істейді. ESP-де қандай трафикті қорғау қажет екенін көрсететін RFT ережесі қолданылған. ESP белсенді күйде.

Команда нәтижесінен 192.168.1.0/24 және 192.168.2.0/24 жеке желілер арасындағы трафиктің шифрланғанын және CORE_1 маршрутизаторынада пакеттің ішіне орналастырылатынын, онда тағайындалған бағыт 210.210.1.2, ал қабылдағыш 210.210.2.2 екенін көре аламыз.

Шығу маршрутизатордың spi 0x60573EF4 (1616330484), ал кіре берісте – 0x6BF362A7 (1811112615). Пакеттер CORE_1 маршрутизаторына түскен кезде, IPSEC модулі SPI, ESP, IP мекенжайларын қарастырады және осы немесе сол ережелерді қолданады және пакетті қауіпсіз арна бойымен өткізуге немесе оның берілмеуі жайлы шешім шығарады. Пакет маршрутизатордан шыққаннан кейін оған SPI 1616330484 қолданылады, бұл мәліметтер маршрутизатордан шығатын пакеттің ESP тақырыбына орналастырылады [1].

Енді IPsec қандай режимде жұмыс істейтінін тексерейік:

```
CORE_1#sh crypto ipsec transform-set
Transform set FIRST: {    { esp-3des esp-sha-hmac  }
   will negotiate = { Tunnel,  },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },
Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },
Router#sh crypto ipsec transform-set
Transform set FIRST: {    { esp-3des esp-sha-hmac  }
   will negotiate = { Tunnel,  },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac
}
   will negotiate = { Transport,  },
Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac
}
   will negotiate = { Transport,  },
```

3.28 сурет – IPsec жұмыс режимін тексеру

CORE_2 маршрутизаторындағы show crypto ipsec командасының нәтижесін көреміз. CORE_2 маршрутизаторына кірген кезде пакет ESP, SPI тексереді және шифрлау, кэштеу және аутентификация алгоритмдерін қолданады:

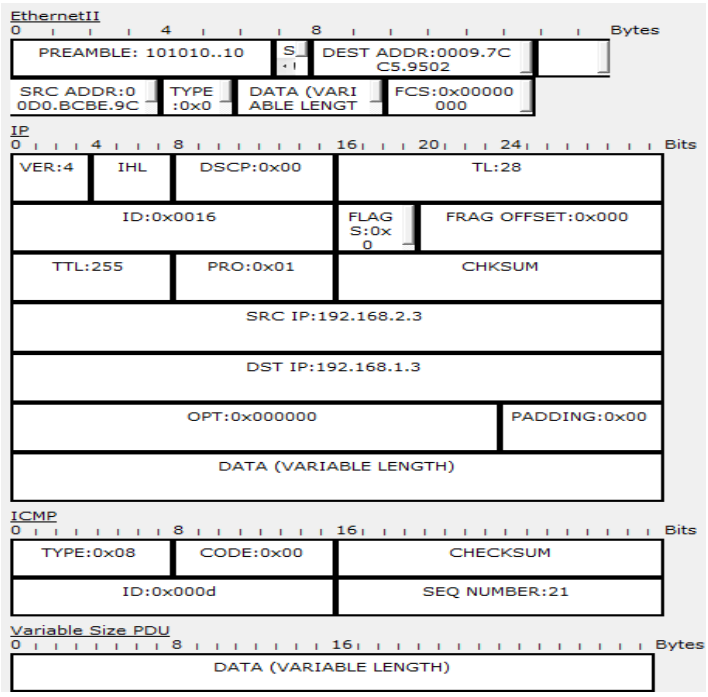
```
local  ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
remote  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
current_peer 210.210.1.2 port 500
 PERMIT, flags={origin_is_acl,}
#pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
#pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

  local crypto endpt.: 210.210.2.2, remote crypto endpt.:210.210.1.2
  path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0/0
  current outbound spi: 0x6BF362A7(1811112615)

  inbound esp sas:
   spi: 0x4408471B(1141393179)
     transform: esp-3des esp-md5-hmac ,
     in use settings ={Tunnel, }
     conn id: 2005, flow_id: FPGA:1, crypto map: RFT
     sa timing: remaining key lifetime (k/sec): (4525504/3570)
     IV size: 16 bytes
     replay detection support: N
     Status: ACTIVE

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
   spi: 0x6BF362A7(1811112615)
     transform: esp-3des esp-md5-hmac ,
     in use settings ={Tunnel, }
     conn id: 2006, flow_id: FPGA:1, crypto map: RFT
     sa timing: remaining key lifetime (k/sec): (4525504/3570)
     IV size: 16 bytes
     replay detection support: N
     Status: ACTIVE
```

3.29 сурет – Маршутизатор ережелері

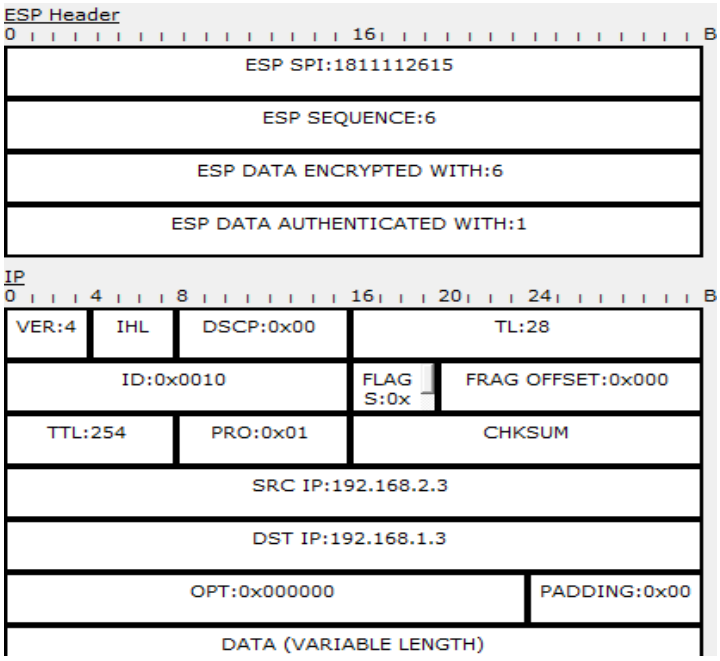
Арнаны қорғаудың бүкіл процесін тексергеннен кейін біз желіде таратылатын пакеттердің мазмұнын қарастырамыз.

Пакеттерді қауіпсіз байланыс арнасы арқылы қалай шифрланғанын және қалай инкапсуляцияға жасалынатынын көрейік. Пакет CORE_1-ге келеді. SA маршрутизаторында ақпарат сканерленеді және пакеттерді шифрлау, инкапсуляциялау мүмкіндігі шешіледі, егер олар осы бірлестіктің ережелеріне сәйкес келсе, онда ESP өңдеу басталады. Пакет байланыс арнасы арқылы 3des протоколы арқылы шифрланады, ал md5 алгоритмі арқылы хэштеу жүреді. Осылайша, пакеттің инкапсуляциясы жүреді және ол IPsec модулінің соңында SPI-мен бірге беріледі. Оған сериялық нөмір беріледі. Содан кейін ол ISP-де қолданылған ережелермен маршрутизатор арқылы жіберіледі. Содан кейін, CORE_2 маршрутизаторында дәл сол процесс жүреді және AS өңдеуі басталады, ал пакет IPsec ережелеріне сәйкес келсе, ESP өңдеу және қауіпсіз арна бойынша беру жүзеге асырылады, оған SPI IPSec модулінің CORE_2 маршрутизаторына кірген кезде қосылады. Қарама-қарсы бағытта берудің бүкіл процесі толығымен ұқсас.

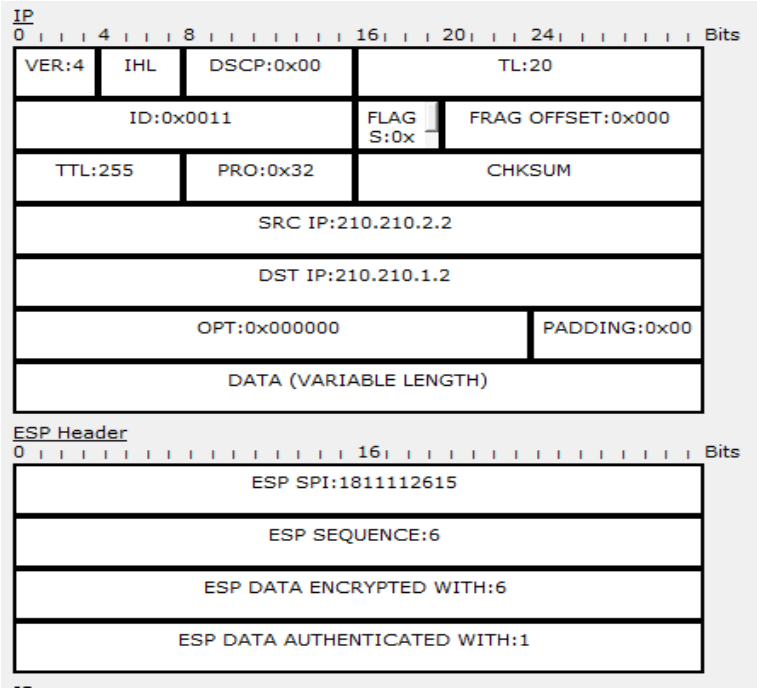
Сонымен пакет 192.168.2.3-дан 192.168.1.3-ға дейін жіберілді:



3.30 сурет - Маршрутизаторға келген таза IP пакеті



3.31 сурет - ESP-өңдеуден кейінгі инкапсуляцияланған деректер

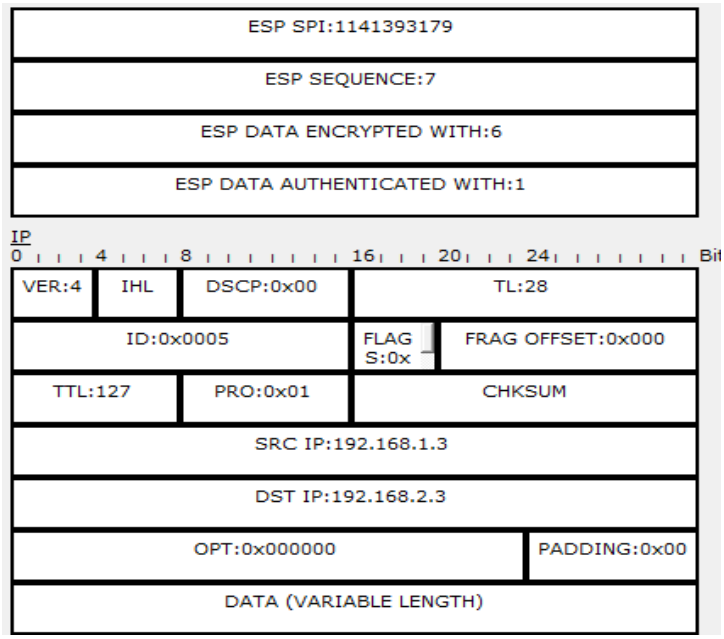


3.32 сурет - Сыртқы IP тақырыбы

Жоғарыдағы 2 суретте біз CORE_2 маршрутизаторына келген пакетті ESP тақырыбымен шығатын IPsec модулінде SPI 1811112615 бар ESP тақырыбымен толығымен инкапсуляцияланғанын көреміз.

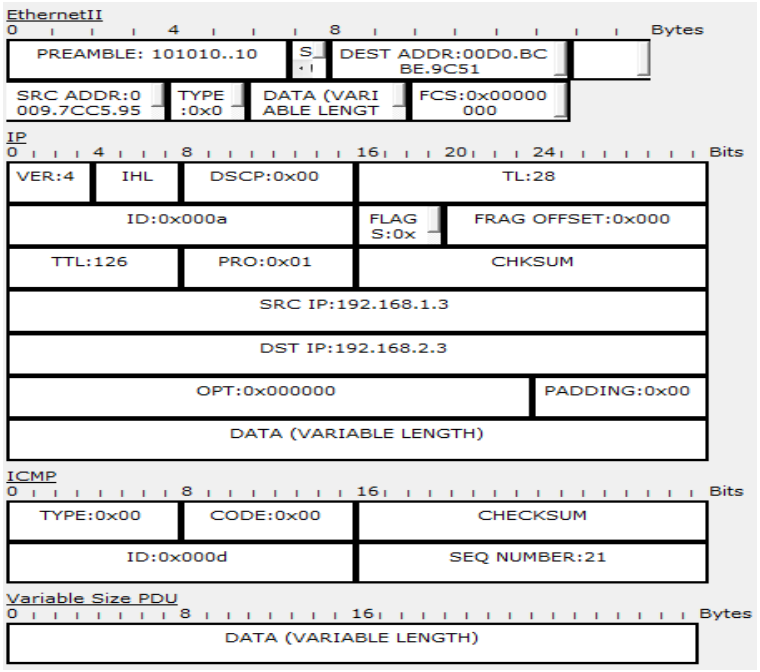
Содан кейін ISP арқылы пакет осындай шифрланған түрде жіберіледі.

CORE_2 арқылы алған кезде пакеттің тақырыбы сақталады және мақсатты түйінге 192.168.1.3 жетеді. Содан кейін осы түйіннен 192.168.2.3-ке ICMP жауабы пайда болады.



3.33 сурет - Кері ICMP жауап бергенде ESP тақырыбы

Белгіленген адреске жеткенде, ол өзінің бастапқы түрінде болады. Төменде белгіленген адреске жеткендегі параметрлері.



3.34 сурет – Қайта шифрланған ICMP-жауап

3.6 Коммутация кестесін MAC-food шабуылынан қорғау

Бұл баптауларды тарату коммутаторларында орындау қажет. Коммутатор интерфейстерінің параметрлеріне кіреміз:

Distribution_1(config)#interface range fastEthernet 0/2-6

Содан кейін port-security функциясын қосамыз:

Distribution_1(config-if-range)#switchport port-security

Содан кейін коммутаторға қосылатын mac-адрестердің санын 100-ге дейін шектейміз [28]:

Distribution_1(config-if-range)#switchport port-security maximum 100

```
Distribution_1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Distribution_1(config)#interface range fastEthernet 0/2-6
Distribution_1(config-if-range)#switchport port-security
Distribution_1(config-if-range)#switchport port-security maximum
100
Distribution_1(config-if-range)#
```

3.35 сурет – Port-security параметрлері

Опцияның арқасында мак-флудтың алдын алу мүмкіндігі пайда болады, оның мақсаты коммутация кестесін толтыру болып табылады.Енді теңшеуге келсек. Мұндай параметрлер екінші коммутаторда да орындалды.

Show port-security address пәрменімен қорғалған MAC адрестерді көруге болады:

```
Distribution_1#show port-security address
                              Secure Mac Address Table
------------------------------------------------------------------------
Vlan       Mac Address Type                          Ports

----       ----------- ----                          -----
10         0060.2F1C.4B01        DynamicConfigured     FastEthernet0/2
11         00E0.8F65.9701        DynamicConfigured     FastEthernet0/3
12         0060.4706.0701        DynamicConfigured     FastEthernet0/4
13         0001.63B6.0D01        DynamicConfigured     FastEthernet0/5
14         00D0.FF69.6401        DynamicConfigured     FastEthernet0/6
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

3.36 сурет – Қорғалған MAC адрестер

3.7 Желілік жабдыққа кіру кезінде есептік деректерді қорғау

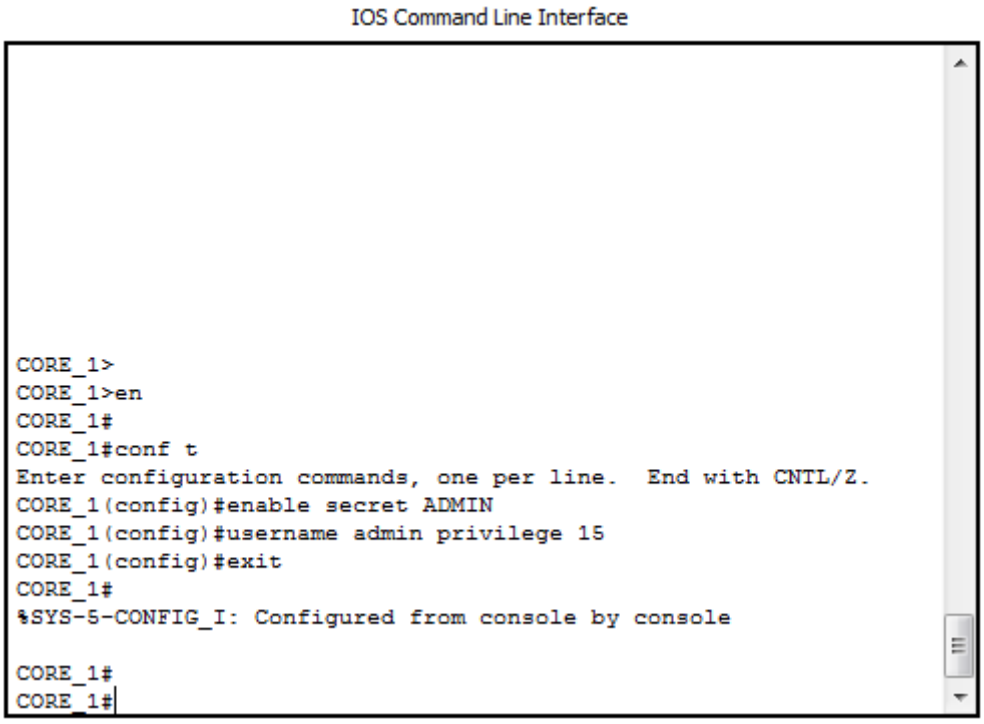
Есептік деректерді қорғау өте маңызды, әсіресе мұндай тармақталған желілер үшін. Сондықтан бұл параметрді орнатамыз.

CORE_1 ядросының маршрутизаторындағы есептік деректерді баптаудан бастайық. Ол үшін артықшылықты режимге кіру үшін парольді теңшеу керек:

CORE_1(config)#enable secret ADMIN

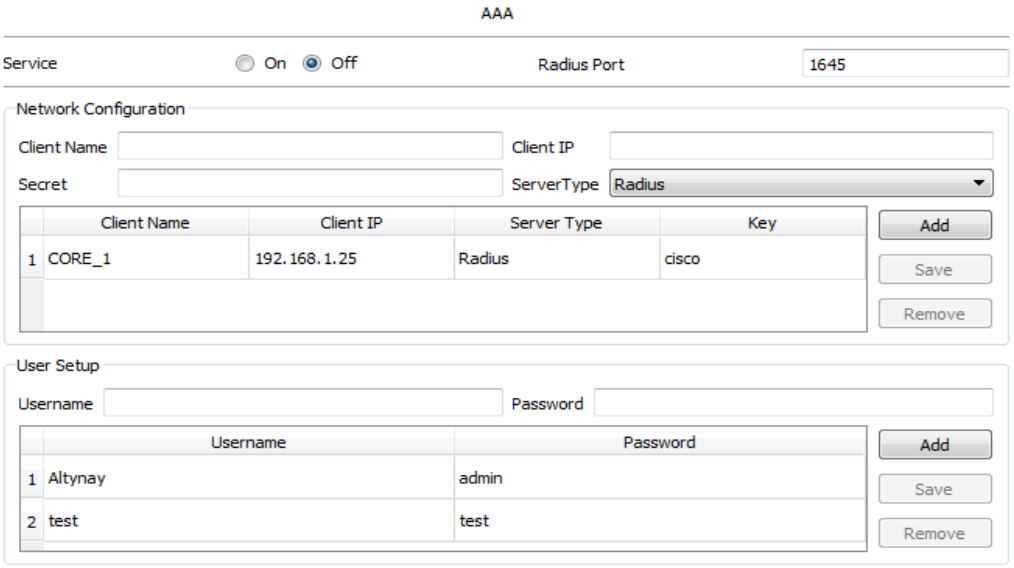
Енді пайдаланушыны баптап, привелегияның ең жоғары деңгейін көрсетеміз-15 орнатамыз:

CORE_1(config)#username admin privilege 15



3.37 сурет – Тіркелгі деректерін теңшеу

Аутентификация үшін серверда RADIUS протоколы қолданылды.



3.38 сурет – RADIUS серверді баптау

Сервер параметрлерінде 2 пайдаланушының тіркелгі деректері орнатылды және осы тіркелгі деректері қолданылатын жабдықтар да көрсетілді.

Аутентификация барлық пайдаланушының есептік деректері бар AAA серверінен өтетін етіп маршрутизаторда келесі параметрлерді жасау керек және оны радиус серверге қолданамыз.

CORE_1(config)#aaa New-model

CORE_1(config)#aaa authentication login default group radius local

Бұл, әдетте, маршрутизаторға RADIUS протоколын қолданып, AAA сервері арқылы қосылады дегенді білдіреді. Егер радиус сервері қол жетімді болмаса, жергілікті тіркелгі деректеріне қол жеткізуге болады [1].

Енді маршрутизаторда радиус серверін орнатуға көшейік:

CORE_1(config)#radius-server host 192.168.1.26 key cisco

```
CORE_1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CORE_1(config)#aaa New-model
CORE_1(config)#
CORE_1(config)#aaa authentication login default group radius
local
CORE_1(config)#
CORE_1(config)#radius-server host 192.168.1.26 key cisco
```

3.39 сурет – RADIUS серверді баптау

Барлық параметрлер аяқталды. Енді қосылымды тексереміз.

```
C:\>TELNET 192.168.1.25
Trying 192.168.1.25 ...Open


User Access Verification

Username: Altynay

Password:
CORE_1>
```

3.40 сурет – Маршрутизаторға қашықтағы құрылғыдан қосылымды тексеру

Осылайша, біз аутентификацияның жұмыс істейтініне және тіркелгі деректерінің қауіпсіздігін қамтамасыз ете алатындығына көз жеткіздік.

4 Өміртіршілік қауіпсіздігі

4.1. Кәсіпорындағы еңбек жағдайларын талдау

Дипломдық жоба барысында «5G желісіндегі ақпараттық қауіпсіздікті талдау» тақырыбы бойынша еңбек жағдайлары қарастырылды.

Пайдалану режимінде 5G желісі қызмет көрсететін қызметкерлердің әрдайым болуын талап етпейді. Бірақ желіге қызмет көрсету кезінде байланыс операторы әрдайым электр тогымен жұмыс істейді. Осыған байланыста жобалық қондырғысы бар аудандағы электр тогының зияндылығына негізінделген есептеулер жүргізілді.

4.1.1 Жерге тұйықтау. Электр тогының адам ағзасына әсері

Жерге тұйықтау – электрқондырғыларының ашық өткізу бөлігінің арнайы байланысы. Қарапайым жағдайда үшфазалы электрсызығында ол кенеусіз болады және генератордың және трансформатордың бейтарап нүктесі жерге тереңірек тұйықталады. Бір фазалық ток кезінде жерге тұйықталған шығу кезінде болады, ал тұрақты ток кезінде – шығу көзінде болады. Жерге тұйықталу электрқауіпсіздікті қамтамасыз ету мақсатында қолданылады.

Жерге тұйықтаушы – тікелей жермен байланыстырылатын және өткізгіштер мен металдардан дайындалатын құрылғы. Жерге тұйықтаушылар жасанды және табиғи болып бөлінеді.

Жерге тұйықтауды өткізуші – жерге тұйықталатын бөлігін жерге тұйықтаушымен жалғастыратын өткізгіш.

Жерге тұйықтаушы құрылғы – жерге тұйықтаушы өткізгіштер мен тұйықтауыштардан конструктивті жалғанатын жиынтық.

Жерге қосу – электрөткізгіштік конструкцияның токөткізгіш бөлігімен жер бетінен оқшауланбаған токөткізбейтін бөлігінің кездейсоқ байланысы.

Корпустағы тұйықталу – электрқондырғының ток өткізбейтін металдық бөлігінің токөткізгіштік арасындағы кездейсоқ қосылысы.

Жерге тұйықтау магистралі – екі немесе одан да жоғары бұтақтарынан тұратын жерге тұйықтау өткізгіші (нөлдік қорғаныс).

Қорғаныстық жерге тұйықтау – жермен немесе оның эквивалентімен кернеуі мүмкін болатын ток өткізбейтін бөлігінің электрлік қосылысы.

Электр тогының адам ағзасына әсері оның әсер ету ұзақтығы мен оның көлеміне байланысты болады. Жерге тұйықтау мақсаты – металдық бұйымдардағы фазалық өткізгіштердің изоляциясының бұзылуы есебінен жоғары кернеуде орналасқан токтың ұруынан адамдарды сақтау.

Жерге тұйықтауды ГОСТ Р 50571.5.54-2013 [30] сәйкес қолдану жағдайлары:

- 380В және одан жоғары номиналды кернеуі бар ауыспалы токты қолдану арқылы және 440В және одан жоғары кернеудегі тұрақты токты пайдалану арқылы жұмыс жасалатын, жоғары қауіптілігі жоқ ғимараттарда;
- МЕМСТ 12.1.013-78 бойынша 42В-380В аралығында номиналды кернеуі бар ауыспалы ток және 110В - 440В аралығындағы тұрақты ток

кезіндегі жоғары қауіптілік пен ерекше қауіптіліктің орын алуы жағдайында жерге тұйықталу қолданылады.

Жерге тұйықталу 1000В дейінгі бейтарап жерге қосылған үшфазалық төртөткізгіштік желілердің тиімділігін көрсетеді.

Жерге тұйықталу жұмыстарының жұмыс принципі – фазаның қысқа тұйықталуын бір корпустағы бірфазалық қысқа тұйықталуға айналдырады, нәтижесінде максималды токтық қорғаныс пайда болады және электр желісінен бұзылған аумақты бөліп алады.

Токтың қорғаныстың пайда болуының шарттары [31]:

$$I_К \geq kI_{НОМ}$$

мұндағы $I_К$ - фазалық өткізудегі қысқа тұйықталу тогы; $I_{НОМ}$ - қорғаныстың қосылуының номиналды тогы; k - қорғаныстық аппаратқа байланысты қысқа тұйықталу тогының қысқаша көрсеткіші; k = 3-6 – балқытушы алдын ала қорғаныштарды қолдану кезінде; k = 1.25-1.4 – автоматты алдын ала қорғауыштарды қолдану кезінде; k =6 – токқа теріс сипаттамасы болатын автоматты алдын ала қорғауыштарды қолдану кезінде.

Нөлдік қорғаныстың өткізгіштері ретінде арнайы осы мақсатқа арналған өткізгіштерді қолдану керек. Өткізгіш сым бойында ажыратылатын қондырғылар мен қорғауыштар болмауы керек. нөлдік өткізгіштер сызығында ажыратушы қондырғыларды қолдануға болады, ол жұмыс істейтін нөлдік өткізгіштермен бірге барлық кернеуде орналасқан өткізгіштерді айыратын жағдайда ғана қолданылады. Генератордың немесе трансформатордың жұмыс жағдайындағы нөлдік өткізгіштің өткізу қабілеті фазалардың шығуында өткізгіштіктің 50% кем емес болуы тиіс. Жыл мезгіліне тәуелсіз токтың бірфазалық көзінің немесе трансформатордың, генератордың жерге тұйықталуының үшфазалық тогының кернеуі 660, 380, 220В кезінде сәйкесінше 2, 4, 8 Ом шамадан аспау керек.

Электрлік берілудің ауа сызықтарында жерге тұйықтау нөлдік жұмыс жағдайында өткізгіш арқылы жүзеге асырылады. Ол фазалық сымдар тартылған бағаналарда орналасады. Нөлдік сымның үзілуі кезінде бір корпусқа фазалардың тұйықталуы қысқа тұйықталудың себебі болып табылмайды және нөлдік сымда ток болмайды.

Нөлдік сымның ажырау орны мен шығу көзіне дейінгі орналасқан қондырғының бейтарап нүктесі нөлге тең потенциалға ие. Ал нөлдік сымның ажырау нүктелерінен тыс орналасқан қондырғы кернеуі жерге қатысты фазалық бөлігіне тең. Бұл кернеу қауіптілік тудырады. Қауіптілікті төмендету үшін нөлдік сымды қайтадан жерге тұйықтау жүргізіледі. Нөлдік сымды қайтадан жерге тұйықтау корпустың жалпы кернеуінің төмендеуімен қатар қашықтықтағы қабылдағыштардың орналасуы кезінде қажет болады. нөлдік сымның қайтадан жерге тұйықталуы 200 м астам ауа сызықтарында және ауа сызықтарынан электрқондырғыларына жер асты тіреулері мен найзағайсіңіргіштер көмегімен өту орындарында жасалынады.

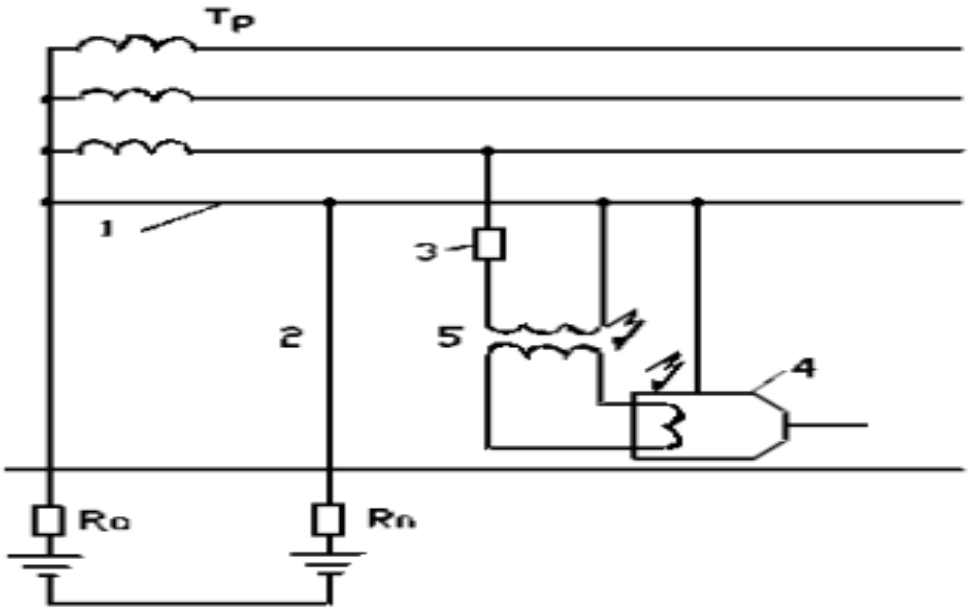
Тұрақты токтың электрсызықтарында нөлдік сымды қайтадан жерге тұйықтау жасанды түрде жүргізіледі. Шарт бойынша олар металдың жер асты құбырларымен жалғанған орны болмауы тиіс.

Жыл мезгіліне тәуелсіз жұмысшы нөлдік сымның қайтадан жерге тұйықтаудың таралуының жалпы кедергісі үшфазалық токтың шығу көзі 660, 380, 220В кернеуі кезінде сәйкесінше 5, 10, 20 Ом көрсеткіштерінен аспауы тиіс. Ал нөлдік жұмысшы сымның қайтадан жерге тұйықталуы таралуының кедергісі 15, 30, 60 Ом шамасынан жоғары болмауы тиіс. Кернеу көрсеткіштері өзгермеді.

4.1.2 Жұмыс жағдайындағы жерге тұйықтау

Лабораторияда көптеген электрқондырғылар бар болатындықтан, яғни серверлер мен компьютерлер, әрі олардың тіреулері металдан жасалғандықтан, ол жерде міндетті түрде жерге тұйықтау болуы тиіс.

Жерге тұйықтау кернеуі төртөткізгіштік электрсызықтарында жерге тұйықтау нейтралының 1000В дейінгісі қолданылады. Жерге тұйықтауды қорғау электрқондырғының зақымдалған жерінің автоматты түрде өшірілуі электрсызығынан немесе кернеуді төмендету арқылы қамтамасыз етіледі. Жоғарыда айтылғандарды қорытындылай келе, жерге тұйықтаудың басты мақсаты корпустағы тұйықталу кезінде токтан максималды қорғау болып табылады. Ол үшін қысқа тұйықталу тогы балқушы құрылғылардың номиналды тогынан бірнеше есе үлкен болуы керек. 4.1 суретте жерге тұйықтаудың принципиалды сызбанұсқасы келтірілген.



Ro – жерге тұйықтаудың бейтарап кернеуі; Rh – адамның есептік кедергісі; 1- жерге тұйықтау магистралі; 2- қайтадан жерге тұйықтау магистралі; 3- өшіру аппараты; 4- электрқондырғы; 5- трансформатор.

4.1 сурет – Жерге тұйықтау сызбанұсқасы

Ток күші қосымша жалғанған кернеу мөлшері мен дене аймағының кедергісіне байланысты болады. дене аймағының кедергісі ішкі мүшелер жасушаларының кедергісінен және тері кедергісінен қалыптасады. Есептеу барысында R = 1000 Ом. Әртүрлі мөлшердегі токтың әсер етуі сайкес, 4.1 кестеде келтірілген [32].

4.1 кесте – Әртүрлі мөлшердегі токтың әсер етуі

Ток,	Адамға әсер етуі	
мА	Ауыспалы ток	Тұрақты ток
0,5	Болмайды	Болмайды
0,6-1,5	Саусақтардың әлсіз дірілдеуі	Болмайды
2-3	Саусақтардың қатты дірілдеуі	Болмайды
5-10	Қолдың тартылуы	Күйдіру
12-15	Сымнан қолды тартып алу қиын	Қатты күйдіру
20-25	Қол біртіндеп жансызданады	Қатты күйдіру
50-80	Тыныс алудың тоқтауы	Тыныс алудың қиындауы
90-100	t>3 сек жоғары – жүректің тоқтауы	Тыныс алу тоқтауы

Оларды қолдану кезінде ауыспалы және тұрақты токтың электрқондырғыларының қауіпсіздік техникасына бірдей талаптар қойылады.

4.2 Есептеу бөлімі

4.2.1 Жерге тұйықтау процесін есептеу әдістері

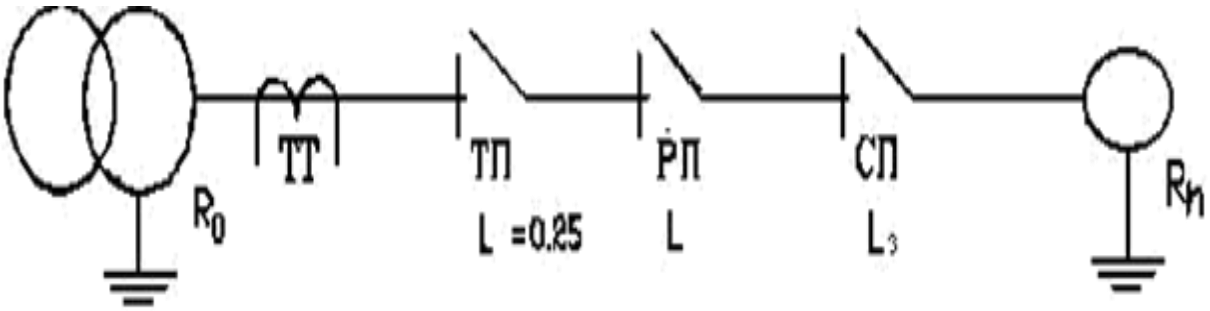
220В номиналды кернеуі бар және 10А номиналды тогы бар электрқондырғыларын нөлге теңестіру жобалануда [33].

Электрқондырғыны қуаттандыру үшін лабораториялық күштік жиынтықты болаттан жасалған түтікшеге орналастырылған АЛП маркалы сым қолданылады. Көлденең қимасы S=2.5мм^2 болатын алюминий өткізгішін таңдаймыз. Тұтынушы магистралдың үшінші бөлігімен жалғастырылған.

Магистралдың бірінші бөлімі полихлорвинилді қабықшада (3 *50 + 1 *25), енді көлденең қимасы бар алюминий сымдары АВРЕ маркалы төртсымды кабельмен орындалған. Бірінші бөлімнің ұзындығы - 0,25 км, $I_{ном}$ = 100А бөлімі токтың А 3110 таратушысы бар автоматпен қорғалған.

Екінші бөлімі ұзындығы 0,075 километр болатын АВРЕ (3 *25 + 1*10) мм кабелімен салынған. Бөлім 80А тогы бар А 3134 автоматты рубильнигімен қорғалған. Магистраль бастапқы кернеуі 6кВ дәне екінші кернеуі 400/220В болатын ТМ=1000 типті трансформатордан қуатталады.

Жерге тұйықтаудың орындалған магистралі алғашқы екі бөлімде қуаттаудың төртінші кабелімен орындалған, ал үшінші бөлімінде – болаттан жасалған түтікше болады.



ТТ – трансформатор; ТП - трансформаторлық подстанция; РП – таратушы пункт; СП – күштік пункт.

4.2 сурет – Энергия көзінің сызбанұсқасы

Қорғаныс үшін ПР-2 тежегіш (қорғауыш) пайдаланылады. Қорғауыш тогы:

$$I_{пр} = \frac{3 \cdot K_П \cdot I_Н}{2,5} = \frac{3 \cdot 10}{2,5} = 12A \quad (4.1)$$

мұндағы: $K_п$ – қосылу коэффициенті = 0,5...4,0;

К коэффициентінің мәні электрқондырғының типіне байланысты алынады:

1. Егер қорғаныс бір электромагниттік уақытша қолдауынсыз, автоматты түрде өшірілу арқылы жүргізілетін болса, К 1,25÷1,4 шамасында алынады.

2. Егер қорғаныс жанып кету уақыты токқа байланысты (ток артқан сайын төмендей бастайды) болатын балқытушы қорғауыштар арқылы жүргізілетін болса, өшіруді жылдамдату мақсатында К ≥3 алынады.

3. Егер ток көзіне кері қосылудың автоматты қорғауыштары қорғалған болса, онда К≥3 алынады.

Стандартты қорғауыш 15А таңдаймыз.

Өйткені сызбанұсқада магистраль бөлімі 20 Ом артық болған жағдайда қайтадан жерге тұйықтау қажет. Жерге тұйықтау кедергісі 10 Ом аспау керек.

4.2.2 Жерге тұйықтау процесінің есептеулерін тексеру

Трансформатор кедергісінің есептік мәнін анықтаймыз.

Фазалық сымның әрбір бөлімінің активті кедергісін есептейміз:

$$R = \rho \frac{L}{S} \quad (4.2)$$

мұндағы: L – сым ұзындығы (м); S – сымның қимасы (көлденең қимасы, мм^2); ρ - материалдың салыстырмалы кедергісі (алюминий үшін ρ=0,028 Ом*мм^2/км).

Фазалық сымның үш бөлімінің активті кедергісін есептейміз:

$$R_1 = 0,028 \cdot \frac{250}{50} = 0,14(Ом) \quad (4.3)$$

$$R_2 = 0,028 \cdot \frac{75}{25} = 0,084(Ом) \quad (4.4)$$

$$R_3 = 0{,}028 \cdot \frac{30}{25} = 0{,}336(\text{Ом}) \quad (4.5)$$

$R_{Ф1}$=0,14(Ом); $R_{Ф2}$=0,084(Ом); $R_{Ф3}$= 0,336(Ом).

Фазалық сымның толық активті кедергісі: $R_{Ф3}$ =0,56(Ом);

Сым температурасын Т=55°С барлық бөлімде бірдей деп қарастырып, температуралық түзетулерді ескере отырып, фазалық өткізудің активті кедергісін есептейміз [34].

$$R_Ф = R_{ФΣ} \cdot (1 + a \cdot (T - 20)) = 0{,}64(\text{Ом}) \quad (4.6)$$

мұндағы: a = $0{,}004^{-1}$ град – алюминийдің кедергі температуралық коэффициенті.

Нөлдік қорғаныстағы сымның активті кедергісі:

$$R_{М\,31} = 0{,}028 \cdot \frac{250}{25} = 0{,}28(\text{Ом}) \quad (4.7)$$

$$R_{М\,32} = 0{,}028 \cdot \frac{75}{15} = 0{,}21(\text{Ом}) \quad (4.8)$$

Болаттан жасалған құбыр үшін: ρ=1,8Ом*$мм^2$/км

$$R_{М\,3} = 1{,}8 \cdot 30 \cdot 10^{-3} = 0{,}054(\text{Ом}) \quad (4.9)$$

Осылайша, жерге тұйықтау магистралінің жалпы кедергісі тең болады:

$$R_{М\,Σ} = R_{М\,1} + R_{М\,2} + R_{М\,3} = 0{,}544(\text{Ом}) \quad (4.10)$$

Фазалық сым үшін ішкі индуктивті кедергісін анықтаймыз.

$$X'_Ф = X'_{ФМ} - X_{ФL} \quad (4.11)$$

Жерге тұйықтау магистралы үшін:

$$X'_М = X'_{ММ} - X_{ML} \quad (4.12)$$

мұндағы: $X'_М$ және $X'_{ФМ}$- индуктивті кедергі, фазалық сымның және жерге тұйықтау магистралының өзара индуктивті жағдайы; $X_М$ және $X_{Ф1}$-өзіндік индукцияның ішкі индуктивті кедергісі.

Индуктивті кедергі, фазалық сымның және жерге тұйықтау магистралының өзара индуктивті жағдайы келесі формула бойынша анықталады:

$$X'_{ФМ} = X'_{ММ} = 0145\lg(d_{ФМ}) \quad (4.13)$$

мұндағы: d – фазалық және нөлдік сымдар арасындағы арақашықтық (1 және 2 d=15 мм үшін, 3 d=9.5 мм үшін)

$$X'_{ФМ1} = X'_{ЖММ} = 0{,}145\ \lg 15 = 0{,}17(\text{Ом}) \quad (4.14)$$

$$X'_{ФМ2} = X'_{ЖММ} = 0{,}145\ \lg 15 = 0{,}17(\text{Ом}) \quad (4.15)$$

$$X'_{ФМЗ} = X'_{ЖММ} = 0{,}145 \lg 9{,}5 = 0{,}142(Ом) \quad (4.16)$$

Барлық территориядағы жалпы кедергі:

$$X'_{ФМ} = X'_{ЖММ} = 3 \square 0{,}145 = 0{,}482(Ом) \quad (4.17)$$

Ішкі индуктивті кедергі келесі формула бойынша анықталады:

$$Ф_L = X'_L L,$$

мұндағы: X'_L- жеке индукцияның салыстырмалы кедергісі, Ом/м.

$$X'_{L1} = 0{,}09 \cdot 0{,}25 = 0{,}023 \text{ (Ом)}$$

$$X'_{L2} = 0{,}068 \cdot 0{,}075 = 0{,}005 \text{ (Ом)}$$

$$X'_{L3} = 0{,}03 \cdot 0{,}03 = 0{,}0009 \text{ (Ом)}$$

Фазалық сымның жалпы ішкі индуктивті кедергісі:

$$X_{ФL} = 0{,}029 \text{ (Ом)}$$

$$X_{ML1} = 0{,}068 \cdot 0{,}25 = 0{,}017 \text{ (Ом)}$$

$$X_{ML2} = 0{,}03 \cdot 0{,}075 = 0{,}0025 \text{(Ом)}$$

$$X_{ML3} = 0{,}138 \cdot 0{,}03 = 0{,}004 \text{(Ом)}$$

Жерге тұйықтау магистралінің жалпы ішкі индуктивті кедергісі:

$$X_{ML} = 0{,}024 \text{ (Ом)}$$

Жалпы ішкі индуктивті кедергі:

$$X'_{Ф} = 0{,}435 - 0{,}0314 = 0{,}453 \text{(Ом)}$$

$$X_{ЖМ}' = 0{,}435 - 0{,}0244 = 0{,}458 \text{(Ом)}$$

Ішкі индуктивті кедергіні анықтаймыз:

$$X_Ф''_{1\text{-}2} = X_{ЖМ}''_{1\text{-}2} = 0{,}057 \cdot 0{,}075 = 0{,}001 \text{(Ом)}$$

$$X_Ф''_3 = 0{,}0157 \cdot 0{,}03 = 0{,}0005 \text{(Ом)}$$

Фазалық сымның және жерге тұйықтау магистралінің толық кедергісі:

$$Z_Ф = 0{,}78 \text{(Ом)}$$

$$Z_M = 0{,}79 \text{(Ом)}$$

Бұл формула бойынша токтың бірфазалығын анықтаймыз:

$$I_{КТ} = \frac{U_Ф}{\frac{Z_Ф}{3} + Z_{ЖМ}} = \frac{220}{0{,}78 + 0{,}79} = 132(А) \quad (4.18)$$

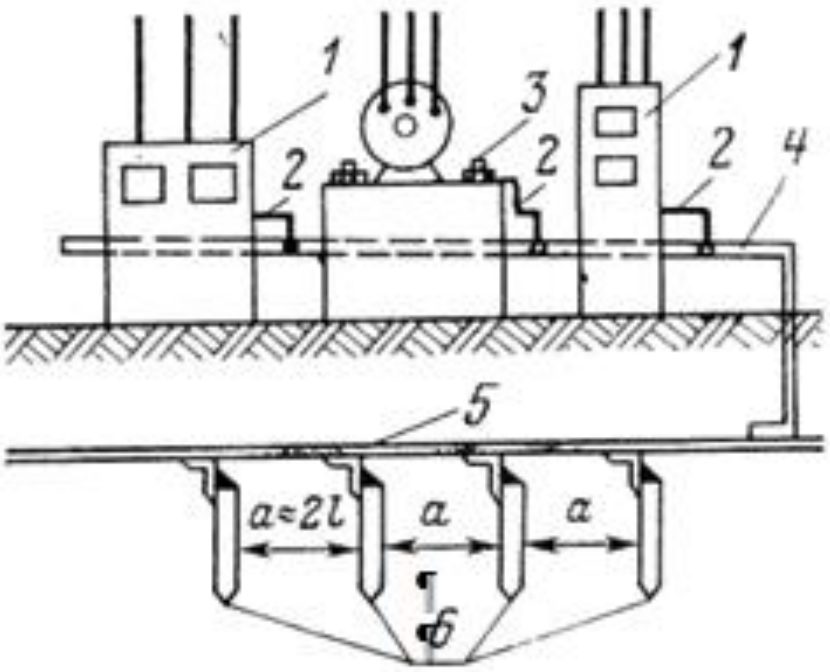
Есептелген көрсеткіш пен рұқсат етілген көрсеткішті салыстырамыз:

$$I_{КЗ} = 132 > 12А$$

Берілген шарттың орындалуын тексереміз.

$$Z_М < 2*Z_Ф$$

Шарт орындалды.



1 - электрқондырғы; 2- жерге тұйықтау өткізгіштері;
3- өткізгіштің орнатылу болты; 4- жерге тұйықтау магистралі;
5- шина контуры; 6- жерге тұйықтаушы (құбыр, бұрыштар).

4.3 сурет – Қорғаныстық жерге тұйықтау конструкциясы

Бөлім бойынша қорытынды: Еңбек жағдайына талдау жүргізілді, негізгі зиянды факторлар анықталды, электр тогының зияндылығын анықтау үшін есептеулер жүргізілді.

5 Ақпараттық қауіпсіздіктің тәуекелдерін есептеу

5.1 Ақпараттық қауіпсіздік тәуекелдерін талдау

Ақпараттық қауіпсіздік тәуекелі - бұл ұйымдағы ақпараттық шабуылдар немесе деректерді бұзу нәтижесінде ақпараттық қауіпсіздікке әсер ету немесе ақпартты жоғалту ықтималдығы. "5G желісіндегі ақпараттық қауіпсіздікті талдау" дипломдық жобасында 5G желісін пайдалану кезінде туындайтын тәуекелдер қарастырдық.

Телекоммуникациялық ұйымдар бүкіл әлемдегі компьютерлерге, желілерге, бағдарламаларға, әлеуметтік желілер мен деректерге тәуелділіктің өсуіне байланысты ақпараттық қауіп-қатерлер үшін неғұрлым осал болып келеді. Мәліметтерді бұзу, кең таралған кибершабуыл бизнеске үлкен теріс әсер етеді және жеткіліксіз қорғалған ақпараттық жүйенің салдарынан жиі туындайды.

Жаһандық қосылу және нашар қауіпсіздік параметрлері бар желілерді пайдалану әсерінен кибершабуыл қаупі артады. Тәуекелдерді басқару және қолжетімділікті бақылау арқылы бұрын шешуге болатын нәрсе енді киберқауіпсіздік, бағдарламалық қамтамасыз ету және киберқауіпсіздік тәуекелдерін басқару саласындағы тәжірибелі кәсіпқойлармен толықтырылуы тиіс.

5.1.1 5G желісінде туындайтын қауіптерді талдау

5G әр түрлі технологияларды біріктіре отырып, мобильді желілер үшін айтарлықтай инновациялар ұсынады. Бұл артықшылықтардың, тәуекелдер мен қауіптер әлі күнге дейін түсініксіз. 5G қауіп-қатерлері IP базасында 5G желісі бар дәстүрлі қатерлерді, 2/3/4G желілірінен қалған қатерлерді және виртуалдау технологиясымен жасалатын қауіптерді біріктіреді.Төменде келтірілген кестеде 5G қауіптерінің жіктелуі көрсетілген:

5.1 кестесі – 5G қауіптерінің жалпы жіктелуі

Атауы	Сипаттамасы
Зиянды қызмет/теріс пайдалану	Көрсетілген мақсатты ұрлау, өзгерту не жою мақсатында зұлымдық әрекеттер арқылы жүйелерге, инфрақұрылымға және қауіпсіздік желілеріне бағытталған болжамды іс-әрекеттер
Тыңдау	Үшінші тараптың коммуникациясын бақылауды келісімінсіз тыңдауға, тоқтатуға немесе басып алуға бағытталған іс-әрекеттер
Физикалық шабуылдар	Инфрақұрылым, жабдық немесе өзара байланыс сияқты физикалық ресурстарды жоюға, бөлшектеуге, өзгертуге, ажыратуға, ұрлауға немесе рұқсатсыз қол жеткізуге бағытталған іс-әрекеттер
Залал	Мүліктің немесе адамдардың істен шығуына немесе пайдалылығын төмендетуге әкеп соғатын әдейі іс-

	әрекеттер
Байқаусызда орын алған залал	Мүліктің немесе адамдардың қирауына, зақымдануына және пайдалылықтың бас тартылуына немесе төмендеуіне әкеп соқтыратын қасақана емес әрекеттер
Ақаулар	Активтің (аппараттық немесе бағдарламалық қамтамасыз етудің) ішінара немесе толық жеткіліксіз жұмыс істеуі
Өшіру	Қызмет көрсетудегі күтпеген іркілістер немесе қажетті деңгейден төмен түсетін сапаның төмендеуі
Апат	Қызметкерлердің едәуір зақым алуына немесе қазасына әкеп соғатын кенеттен болатын авария немесе табиғи апат

Жоғарыда аталған жалпы таксономияға қосымша, біз сондай-ақ пайдалану мақсаты базалық желінің, радиоқолжеткізудің, желіні виртуалдандырудың немесе жалпы инфрақұрылым компонентінің бөлігі болып табылатындығына байланысты қауіптерді жіктейміз. Осы критерийге сүйене отырып, 5.2 кесте құрылды.

5.2 кестесі – 5G қауіптерінің жіктелуі

Атауы	Сипаттамасы
Базалық желінің қатері	Бұл қатерлер 5G базалық желісінің элементтеріне жатады және олардың көпшілігі "теріс пайдалану" және "тыңдау" санатына жатады
Қатынау желісінің қауіп-қатері	Бұл қатерлер 5G радиоқатынау технологиясына жатады. Көптеген қауіп-қатерлер "тыңдау/ұстап қалу" санатынан
Бірнеше есептеулердің қатерлері	Бұл қатерлер желі шекарасында орналасқан компоненттерге жатады. Олардың көпшілігі "теріс пайдалану" және "тыңдау /ұстап алу"санатына жатады
Виртуализация қауіптер	Бұл базалық ақпараттық технологиялар инфрақұрылымын, желілер мен функцияларды виртуалдандыруға байланысты қауіптер
Физикалық инфрақұрылымның қатері	Бұл желіні қолдайтын базалық ақпараттық технологиялар инфрақұрылымына байланысты қауіптер. Олардың көпшілігі "физикалық шабуылдар", "жабдықтың зақымдануы немесе жоғалуы", "жабдықтың істен шығуы немесе ақаулығы", "өшірілуі", "апат"санатына жатады
Жалпы қауіптер	Бұл әдетте кез келген жүйеге немесе ақпараттық қауіпсіздік технологиялар желісіне әсер ететін қауіптер. Мысалы, 5G көптеген ерекше қатерлер желілік қызметті ажыратуға әкелуі мүмкін, бұл жалпы белгілерде қызмет көрсетуден бас тарту қаупі (DoS).

5.1 сурет – 5G желісінің қауіп-қатерлері

5.1.2 5G желісінің активтері

Ақпараттық қауіпсіздік тәуекелдерін талдау үдерісі активтерді анықтаудан басталады. Актив – адам немесе ұйым үшін құндылығы бар және сондықтан қорғауды талап етеді. Ұйым үшін құндылықтан басқа, активтер заңды міндеттемелерді орындауға ықпал етуі мүмкін.

Ақпараттық қауіпсіздіктің типтік жүйесінде активтер:

а) аппараттық, бағдарламалық және коммуникациялық компоненттер;

б) олардың арасындағы коммуникациялық байланыстар;

с) жүйенің функциясын бақылайтын, ол өндіретін және тұтынатын немесе оған түсетін деректер;

d) физикалық және ұйымдық инфрақұрылым, жүйе (біздің дипломдық жобамыз бойынша 5G);

е) жүйемен өзара әрекеттесетін және оның жұмысына әсер етуі мүмкін адам агенттері (мысалы, пайдаланушылар, жүйелік әкімшілер және т.б.).[1]

5G активтер диаграммасы олардың қауіптерге ұшырауына сәйкес активтер топтарын пайдалана отырып құрылымдалған. Активтердің құпиялық, қол жетімділік және тұтастықтың қауіпсіздігімен байланысты қасиеттерін қолдаудағы рөлін назарға ала отырып, олардың маңыздылығын бастапқы бағалау әзірленді. Бұл ретте 5G инфрақұрылымының жалпы қауіпсіздігі мен қол жетімділігін қолдауға жауап беретін және кибершабуылдардың белгілі мақсаттары болып табылатын активтер топтарына баса назар аударылды.

Активтердің категориялары 5.2-суретте көрсетілген, ал олардың мазмұны келесідей:

Саясат. Саясатты басқару функциялары тұтынушының функцияларына байланысты сеанстарды бастамалауды, басқаруды жүзеге асырады. Олардың тұтынушылармен байланысты саяси мәселелерді басқарудағы рөлін ескере отырып, бұл функциялар 5G желісін пайдалану үшін қаржылық мәселелерге (төлем есептеу) ықпал етуге бағытталуы мүмкін.

Басқару процестері. Активтердің осы тобы 5G инфрақұрылым құрауыштарының барлық жиынтығын әзірлеуге, өрістетуге және пайдалануға арналған маңызды процестерді жинақтайды.

Бизнес-қосымшалар. Алдыңғы буынның мобильді желілеріне ұқсас, бұл активтер 5G желісінде бизнеске байланысты мәселелерді іске асыру үшін қажет клиенттермен қарым-қатынасты басқару және пайдалануға беруді білдіреді.

Бизнес-сервистер. 5G контекстінде активтердің осы тобы нақты қызметті ұсыну үшін қажетті компоненттерге жатады. Мысал көлденең, іскерлік, үкіметтік, сыни және шұғыл қызметтерді ұсыну болып табылады.

Хаттамалар. Бұл активтер тобы 5G инфрақұрылымында пайдаланылатын (негізгі) коммуникациялық хаттамаларды ұсынады.

Деректер беру желісі. Активтердің осы тобы сыртқы деректерге, контентке, қызметтерге және 5G желісінен тыс қолжетімді басқа ресурстарға қосылуды ұсынады.

Тәуелсіз логикалық желілер. Активтердің бұл тобы бөліктерді құру мен басқаруға жауапты 5G барлық функцияларын ұсынады. Бөліктер – бұл виртуализацияланған тәуелсіз логикалық желілер, олар пайдаланушы жабдығы мен 5G қызметтері арасында желі байланысын жүзеге асырады.

Деректер. Активтердің бұл тобы 5G жұмыс істеу үшін барлық деректерді қамтиды, әсіресе құпия және қауіпсіздікпен байланысты 5G деректер.

Адами активтер. Активтердің ең маңызды топтарының бірі болып есептелетін адами активтер 5G желісін пайдалануға және пайдалануға тартылған барлық тұлғаларды білдіреді.

Уақыты. Уақытқа байланысты көптеген функцияларда маңызды рөл атқарады (мысалы, қызмет көрсету сапасы, желіні басқару, виртуалдандыруды басқару және т.б.). Уақыт пен желілік функциялар арасындағы аса сыни өзара іс-қимыл қауіпсіздік функцияларына (кілттерді басқару, шифрлау және уақытша белгілер сияқты) қатысты. Уақыт бойынша дәлсіздіктер желілік функциялардың қол жетімділігі үшін алыс болатын салдарлар болуы мүмкін іркілістер мен манипуляцияларға әкелуі мүмкін. Айта кету керек, 5G-да уақытша дәлсіздіктердің қысқаруы қазіргі 5G виртуализация тәжірибесі мен спецификацияларында әлі толық ескерілмеген.

Заңды активтер. Осы санаттағы активтер әртүрлі келісім-шарттық келісімдермен және зияткерлік меншік құқықтарымен байланысты, олар не түрлі мүдделі тараптар арасында екі жақты қызмет көрсетудің нысанасы болып табылады, не пайдаланылатын қызметтер мен компоненттерге зияткерлік меншік құқықтарымен байланысты.

Мұрагерлік активтер. Активтердің бұл тобы 5G желісіне қосылған немесе косылу жолдарында пайдаланылатын (мысалы, 2G-дан 5G-ға дейін) барлық ескірген жүйелерді қамтиды.

Деректер қоймасы. Бұл актив 5G сақталатын деректерге тұрақты және қол жеткізуді қамтамасыз ететін барлық активтерді (негізінен желілік функцияларды) қамтиды.

5.2 сурет – 5G активтердің пайдаланылатын санаттары

Келесі кестеде біз активтердің сәйкестендірілген топтарының өзектілігін келтіреміз.

5.3 кестесі – Активтердің сәйкестендірілген топтарының өзектілігі

Активтер тобы	Құпиялылық	Тұтастық	Қолжетімділік
Саясат	🟡	🟡	🔵
Басқару процестері	🟡	🟡	🟡
Бизнес-қосымшалар	🔴	🔴	🟡
Бизнес-сервистер	🟡	🟡	🟡
Хаттамалар	🔵	🔴	🟡
Деректер беру желісі	🔵	🔵	🟡
Тәуелсіз логикалық	🔵	🔵	🔴

желілер			
Деректер	●	●	●
Адами активтер	●	●	●
Уақыты	●	●	●
Заңды активтер	●	●	●
Мұрагерлік активтер	●	●	●
Деректер қоймасы	●	●	●

Шартты белгілер:

Қасиеттерді қолдау үшін активтер тобының өте жоғары релеванттылығы: ●

Қасиеттерді қолдау үшін активтер тобының жоғары релеванттылығы: ●

Қасиеттерді қолдау үшін активтер тобының орташа релеванттылығы: ●

Қасиеттерді қолдау үшін активтер тобының төмен релеванттылығы: ●

Қауіпсіздіктің осы қасиеттерінің бекітілуі активтер тобы деңгейінде орындалды. Бұдан әрі қатерлерді бағалау дәлдігі үшін бірнеше активтерді егжей-тегжейлі қарастырайық.

5.4 кесте – Активтер тізбегі

Активтер			
№	Атауы	Сана	Активтің коды
1	Деректер (пайдаланушылардың, қосымшалар, қауіпсіздік, желілік)	1	dat
2	Қауіпсіздікті басқару құралдары	1	sec
3	Бұлт, виртуализация	1	vir
4	Базалық станция	1	ser
5	Конфигурация деректері (жүйелер, желілер, қауіпсіздік)	1	kon

5.2 Есептеу бөлімі

5.2.1 Екі параметр бойынша тәуекелдерді бағалау

Дипломдық жобаның ақпараттық қауіпсіздік тәуекелдерін бағалау үшін екі праматетр бойынша тәуекелдерді бағалау әдісі таңдалды. Екі параметр бойынша тәуекелді бағалау әдісі қауіптің туындау ықтималдығын бағалауды және ықтимал залалды бағалауды қамтиды.

Осы әдістеме бойынша тәуекел 5.1 формуламен анықталады

Тәуекел ағымдағы= Пайда болу ықтималдығы х залалды бағалау (5.1)

Бұл әдіс үш кезеңді қамтиды:

а) тәуекелдердің бастапқы есебі

б) үлкен тәуекелдерге арналған шараларды айқындау

в) қайта есептеу

Тәуекелдердің бастапқы есебі қауіптің туындау ықтималдығын және ықтимал залалды анықтаудан басталады.

Қауіптің туындау ықтималдығын анықтау үшін 5.3-кестені пайдалану қажет, онда есептеу үшін қауіптің туындау ықтималдығының мәні және оның уақыт арақатынасы сипатталған.

5.5 кесте – Значение вероятности возникновения угрозы

Қауіптердің туындау ықтималдығы шкаласы	
Ықтималдылық деңгейі	Қауіптің туындау ықтималдығы
0-өте төмен	Шамамен 2-3 рет 10 жылда
1-төмен	Шамамен 5 жылда бірнеше рет және сирек
2-орташа	Шамамен жылына бірнеше рет
3-жоғары	Айына шамамен 1 рет
4-өте жоғары	Шамамен айына бірнеше рет

Мүмкін болатын залалды анықтау үшін 5.4-кестені пайдалану қажет, онда есептеу үшін залалдың мәні және оның ақшалай баламадағы арақатынасы сипатталған.

5.6 кесте – Залалдың мәні және оның ақшалай баламадағы арақатынасы

Шығын көлемінің шкаласы	
Мәні	Сипаттамасы
0-өте төмен	құны 50 000 теңгеге дейін
1-төмен	құны 200 000 теңгеге дейін
2-орташа	құны 500 000 теңгеге дейін
3-жоғары	бағасы 1 000 000 теңгеге дейін
4-өте жоғары	құны 1000 000 теңгед

Тәуекелдерді бағалау нәтижелері 5.5 қорытынды кестеге енгізілді.

5.7 кесте – Екі параметр бойынша есептеулердің нәтижесі

№	Тәу-л коды	Қауіптер	Осалдық	Тәуекелдің ең жоғары деңгейі	Тәуекелді өңдеу жөніндегі шаралардың атауы	Тәуекелдің қалған деңгейі
Деректер (пайдаланушылардың, қосымшалар, қауіпсіздік, желілік)						
1.1	aa	Деректерді түрлендіру	Қол жеткізу құқықтарын дұрыс бөлмеу	6	Қолжетімділікті шектеу, парольдік қорғауды ұйымдастыру	4
1.2	bb	Құпия ақпаратты ашу және оқу	Күрделі ақпаратты шифрленбеген түрде сақтау	6	Серверлерде сақталатын деректерді қорғауға арналған криптографиялық шешімдер кешені	4
1.3	cc	Құпия деректерді жария ету	Қызметкерлер біліктілігінің төмен деңгейі	4	Қолжетімділікті шектеу, парольдік қорғауды ұйымдастыру	2
Қауіпсіздікті басқару құралдары						
2.1	dd	Қауіпсіздік саясатының құпия бөлігін жария ету	Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметкерлер біліктілігінің төмен деңгейі	4	Қауіпсіздік саясатын білу талаптары мен біліктілігін үнемі арттыру	2

2.2	ee	Қауіпсіздікті қамтамасыз етудің арнайы бағдарламалық құралдарының істен шығуы	Бағдарлама жұмысының параметрлеріне өзгерістер енгізуді тиімді бақылау кемшіліктері	6	Тұрақты тексеру үшін БҚ пайдалану зиянды БҚ болуы және жүйені жаңарту	4
2.3	ff	Рұқсатсыз қол жеткізу және бағдарламалардың жұмысын бұзу	Қол жеткізу құқықтарын дұрыс бөлмеу	3	Қолжетімділікті шектеу, парольдік қорғауды ұйымдастыру	3
Бұлт, виртуализация						
3.1	gg	Деректерді жоғалту	Сақтық көшірме жасау процедурасынан алынғандар	3	Тұрақты жүйелік көшіру және сақтау жүйесін теңшеу	3
3.2	hh	Деректерді ұстап қалу және түрлендіру	Жеткізуші мен ресурсының IP-мекенжайын ауыстыру мүмкіндігі	4	Деректерді шифрлау, алушыны аутентификациялау	2
Базалық станция						
4.1	kk	Базалық станцияларға рұқсатсыз физикалық қол жеткізу	Арнайы бағдарламалардың көмегімен авторландырудан өтпей, құпия ақпаратты алу мүмкіндігі	4	Қолжетімділікті шектеу, парольдік қорғауды ұйымдастыру	2

4.2	ll	Пайдаланушылардың жеке деректерін жоғалту, ұрлау	Сенімді қорғаудың болмауы және қолжетімділікті шектеу	4	Қолжетімділікті шектеу, парольдік қорғауды ұйымдастыру	2
4.3	zz	Рұқсатсыз әрекеттер / желіге кіру	Желі қауіпсіздігі тетіктерінің болмауы немесе дұрыс орнатылмауы	3	Желіні қорғауды ұйымдастыру	3
Конфигурация деректері (жүйелер, желілер, қауіпсіздік)						
5.1	xx	Маршруттау кестелерін манипуляциялау	Желі парольдеріне және маршрутизатордың жеке кабинетіне кіру	3	Күрделі парольдер, тұрақты жаңарту	3
5.2	cc	Конфигурация деректерін бұрмалау	Сенімді қорғаудың болмауы және қолжетімділікті шектеу	4	Қолжетімділікті шектеу, парольдік қорғауды ұйымдастыру	2
5.3	vv	Дұрыс орнатылмаған жүйені / желіні пайдалану	Желідегі жұмыс бойынша мамандардың біліктілігінің төмен деңгейі	6	Желі мен жаңартуларды тұрақты тексеру	3
5.4	nn	Зиянды желілік функцияларды тіркеу	Желі парольдеріне және маршрутизатордың жеке кабинетіне кіру	6	Күрделі парольдер, тұрақты жаңарту	4

5.2.2 Ақпараттық қауіпсіздік тәуекелдерін CORAS әдіснамасымен талдау

Қазіргі уақытта ақпаратты қорғау проблемасы мобильді байланыс технологиясының таралуына байланысты аса өткір сипатқа ие болды. Мобильді кәсіпорынның ақпараттық қауіпсіздік тәуекелдерінің төмендеуі кез келген бизнестің өзекті және басты міндеттерінің бірі болды. Тәуекелдерді талдау және басқару мобильді кәсіпорынның қауіптерін, осалдығын және тәуекелдерін бағалауға, сондай-ақ жеткілікті қорғау деңгейін қамтамасыз ететін қарсы шамаларды анықтауға мүмкіндік береді.

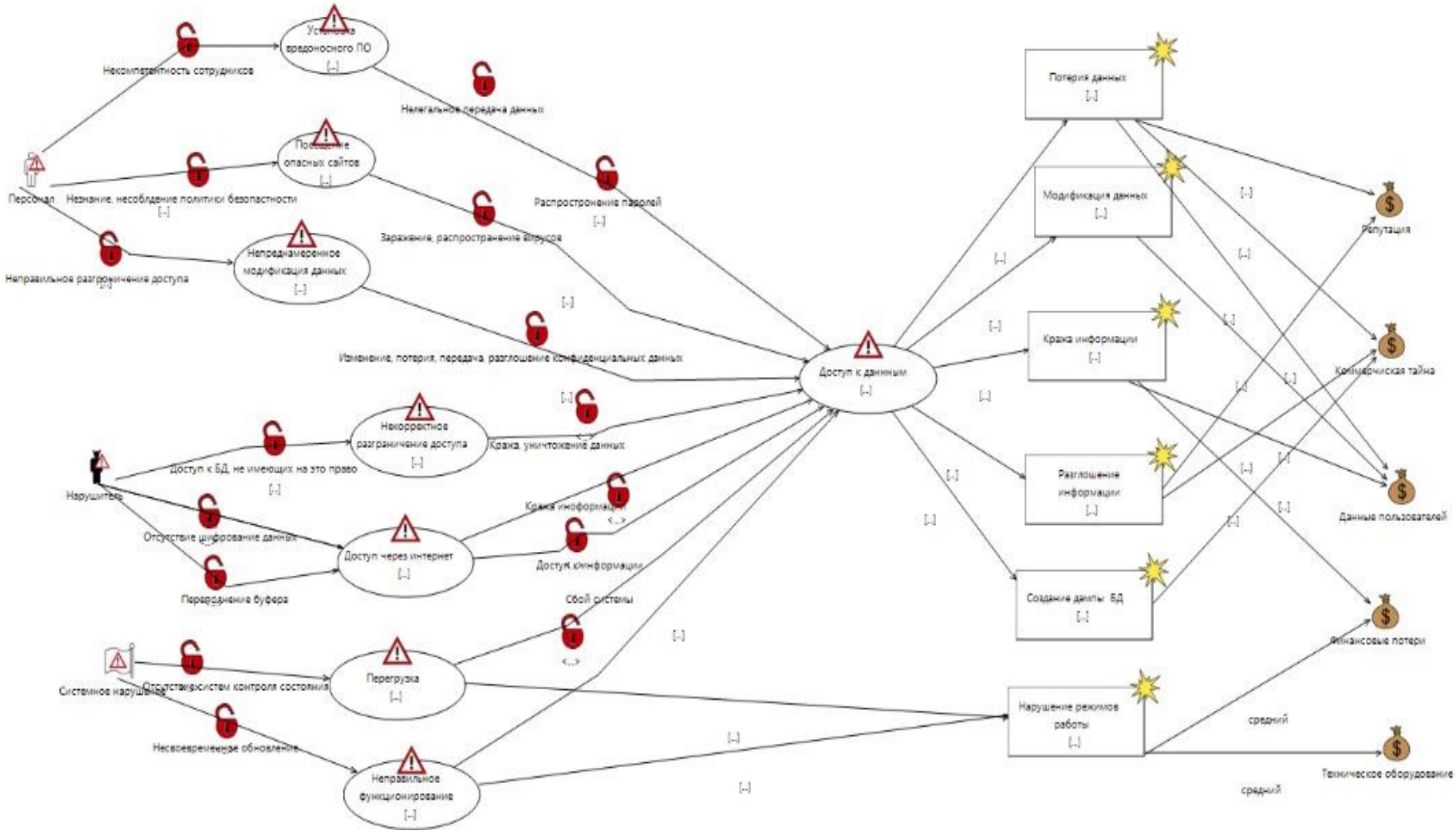
Қауіпсіздік тәуекелдерін талдауға арналған Coras әдіснамасы бүкіл жұмыс барысында қолданылатын тәуекелдер мен қатерлерді модельдеу құралы болып табылады. UML тілін қолданады (ағылш. Unified Modeling Language-модельдеудің біріздендірілген тілі) - бағдарламалық қамтамасыз ету саласындағы объектілі модельдеуге арналған графикалық сипаттама тілі. UML-кең профиль тілі, бұл UML-модель деп аталатын жүйенің дерексіз моделін жасау үшін графикалық белгілерді пайдаланатын ашық стандарт. UML анықтау, визуализация, жобалау және құжаттау, негізінен бағдарламалық қамтамасыз ету үшін жасалды.

CORAS бағдарламасын қауіпсіздік тәуекелдерін талдау үшін пайдаланамыз:

Қауіпсіздікті талдау ең алдымен активтерді анықтаудан басталады. Қорғауға жататын ақпаратты анықтаймыз, яғни компанияның негізгі активтерінің өзара байланысын бағыт көрсеткісі көмегімен бейнеледік (5.2-кесте).

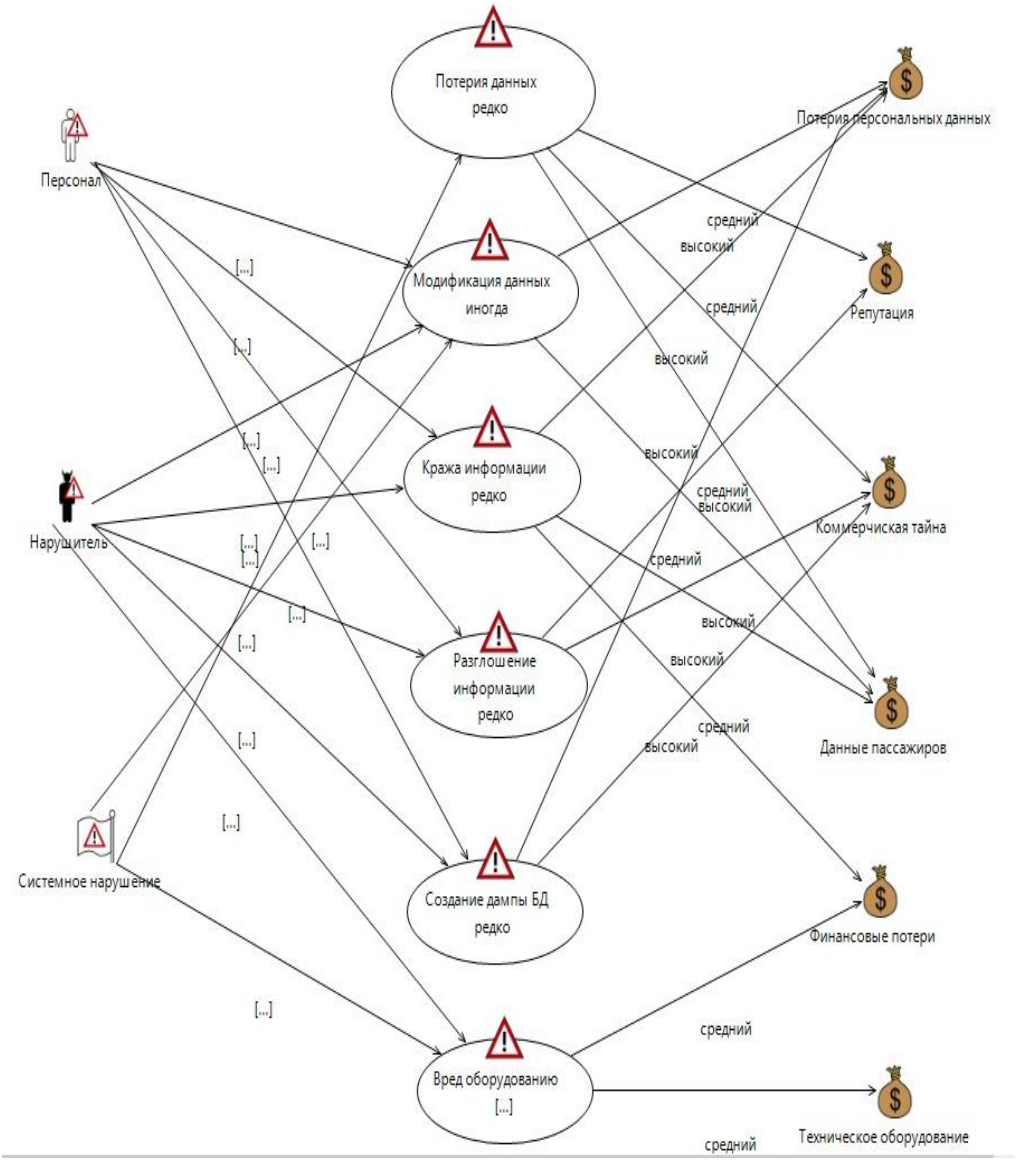
5.3 сурет – Активтар

Пайда болу факторы бойынша қауіптер диаграммасын құру қажет: адам факторымен байланысты (әдейі және әдейі емес) және адам факторымен байланысты емес. Қауіптердің тууына себеп болатын осалдықтар мен осы қауіп әсерінен зиян келетін факторды бейнеледік.



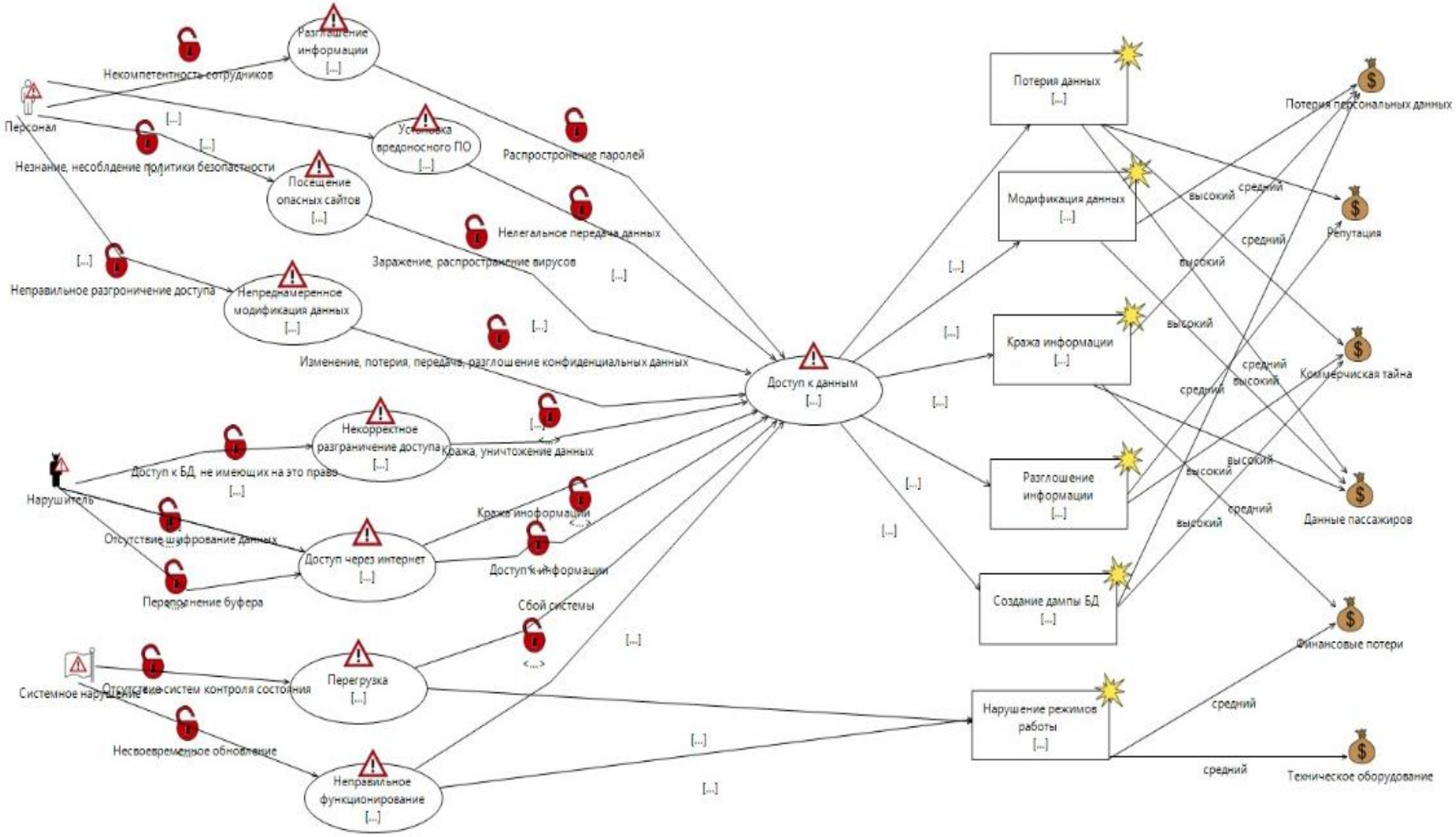
5.4 сурет – Қауіптер диаграммасы

Қандай тәуекелдер аса қауіпті екенін анықтау үшін тәуекелдер диаграммасын құру қажет. Қауіптерді пайда болу көздерімен байланыстырамыз, орын алған қауіптердің зиян келетін факторларға қаншалықты әсер етеінін бейнеледік.



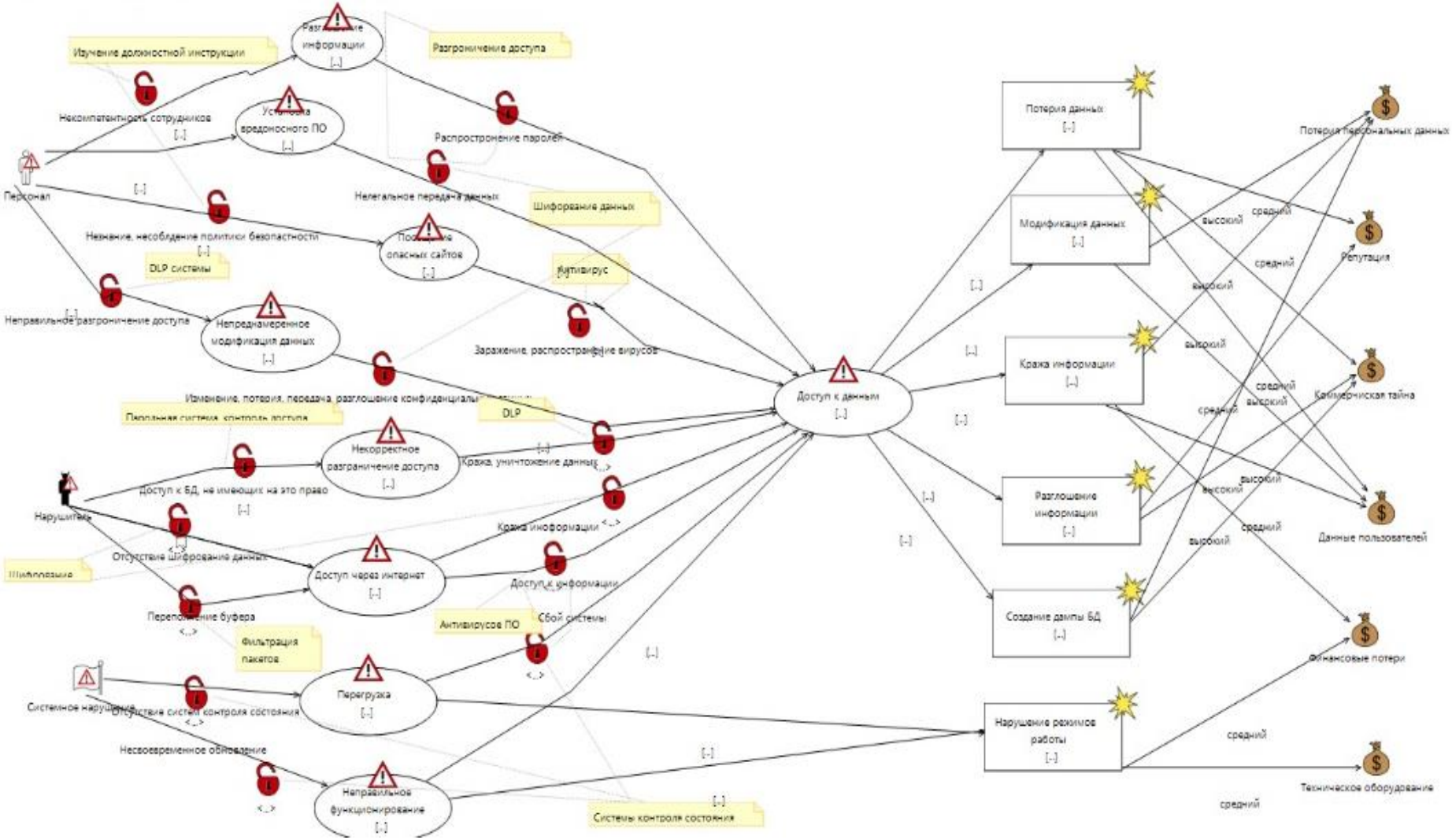
5.5 сурет – Тәуекелдер диаграммасы

Бұдан әрі тәуекелдердің жиілігіне қарай даралау үшін ықтимал сипаттамалары бар диаграмма салу қажет. Жоғарыдағы екі диаграмманы біріктіреміз. Қауіптердің орын алу жиілігі мен әсер етуші факторын, туу көздерін бірге бейнеледік.



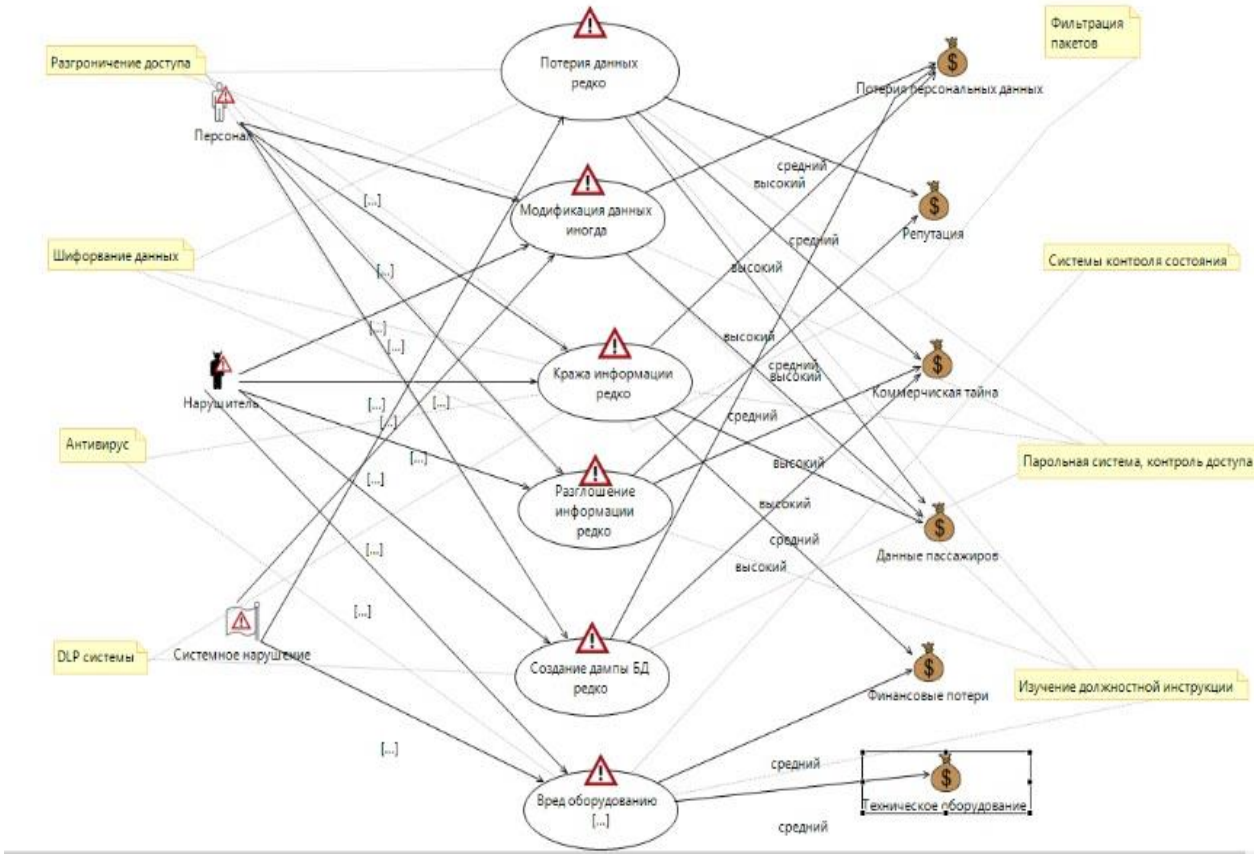
5.6 сурет – Ықтимал сипаттамалары бар қауіптер диаграммасы

Бұдан әрі жол берілмейтін тәуекелдер үшін қарсы әрекет диаграммасын құру қажет. Қауіптер диаграммасында әрбір осалдыққа қарсы әрекет етеміз. Нәтижесінд туу көзі, қауіп, туу ықтималдығы, оалдық және әсер етуші факторы бар толық диаграмма алдық.



5.7 сурет – Қорғау элементтері бар қауіптер диаграммасы

Қорытындысында тауекелдердің орын алу жиілігі мен орын алған жағдайда әкеп соғатын қатерімен, тәуекелдің алдын алу шараларымен бірге диаграмма құрамыз.



5.8 сурет - Қауіпті тәуекелдер диаграммасы

Бөлім қорытындысы. Бұл бөлімде біз ақпараттық жүйенің осалдығын анықтау және оларды жою мақсатында тәуекелдердің есебін жүргіздік. Тәуекелдерді есептеу әдістің негізінде екі параметр бойынша жүргізілді. Есептеу нәтижелері ақпараттық жүйенің ағымдағы жағдайын анық көруге мүмкіндік береді. Бұдан әрі бұрын есептелген тәуекелдерді төмендетуге бағытталған қорғау құралдары енгізілді. Тәуекелдерді төмендету үшін қажетті ақпаратты қорғау жүйесі анықталғаннан кейін тәуекелдерге сол әдіс бойынша қайта есептеу жүргізілді. Енгізуге ұсынылатын қорғау шараларын немесе қорғау жүйелерін ескере отырып, тәуекелдерді қайта есептеу нәтижесінде олар қолайлы деңгейге дейін төмендеді. Тәуекелдерді есептеудің осы әдістері шын мәнінде пайдалы болып табылады және ақпаратты қорғауға қатысты ақпараттық жүйенің ағымдағы жағдайын көруге мүмкіндік береді.

ҚОРЫТЫНДЫ

Дипломдық жоба аясында ақпараттық қауіпсіздікке талдау жасалып, ұялы жүйелердің соңғы буындары арасында салыстырмалы параллель жүргізілді. Желілердің ақпарттық қауіпсіздік қатерлерінің ұқсастықтар мен айырмашылықтар анықталды.

Мобильді желілердің болашақ архитектурасы үшін ең перспективалы радиоқатынау желілері (CRAN), бағдарламалық-анықталатын желілер (SDN) және желілік функциялардың виртуализациясы болып табылады. Екінші жағынан, SDN және NFV желілері желілік басқару талаптарына сәйкес желілік функцияларды бағдарламалау мен басқаруда икемділікті ұсына алады.. CRAN архитектурасы осы жұмыс үшін қарастырылады, өйткені ол өз сипаттамаларына байланысты келесі 5G ұялы желілерінің негізгі бөлігі болып табылады. Архитектураның жаңа шешімдері жалпы жұмыс үшін пайдалы болғанымен ақпараттық қауіпсіздік талаптары мінсіз емес. Олардан бөлек байланыс арналарындағы, мобильді желі бұлтты сервисіндегі ақпараттық қауіпсіздік мәселелеріне талдау жасалды және шешімдері көрсетілді.

Тәжірибелік бөлімде Cisco Packet Tracer симуляторында 5G желісінің сұлбасы жобаланды. Ең алдымен, жүйенің жақсы жұмысы үшін IP-адресация мен VLAN-дар қатынау деңгейіне дейін бапталып, DHCP және NAT пен күйге келтірілді. Қауіпсіздікті қамтамассыз ету мақсатында ESP - 3DES-шифрлау әдісі, MD5-хэштау алгоритмі, құпия кілттермен алмасудың Диффи-Хеллман әдісі, ISAKMP саясаты, кеңейтілген ACL, IPSec Transform, криптографиялық карта іске асырылды.

Пайдалану режимінде 5G желісі қызмет көрсететін қызметкерлердің әрдайым болуын талап етпейді. Бірақ желіге қызмет көрсету кезінде байланыс операторы әрдайым электр тогымен жұмыс істейді. Осыған байланыста жобалық қондырғысы бар аудандағы электр тогының зияндылығына негізделген есептеулер жүргізілді.

Ақпараттық қауіпсіздік тәуекелдерін бағалау бөлімде ақпараттық жүйенің осалдығын анықтау және оларды жою мақсатында тәуекелдердің екі параметр бойынша есебі жүргізілді, тәуекелдерді төмендетуге бағытталған қорғау құралдары енгізілді және қайта есептеу жүргізілді. Енгізуге ұсынылатын қорғау шараларын немесе қорғау жүйелерін ескере отырып, тәуекелдерді қайта есептеу нәтижесінде олар қолайлы деңгейге дейін төмендетілді.

Дипломдық жоба 5G желісінің ақпараттық қауіпсіздігіне талдау жасалып, негізгі осалдықтар сипатталды және оларды шешу жолдары көрсетілді. Практикалық мақсатта қолдануға болатын 5G желісінің прототипі құрылды.

Қысқартулар тізбесі

5G – сымсыз телефон технологиялары мен мобильді телекоммуникациялардың бесінші буыны (ағылш.5 – Generation).

IP мекен-жай – компьютерлік желідегі тораптың бірегей желілік мекенжайы (ағылш. Internet Protocol Address).

IoT – интернет арқылы байланысқан, деректерді жинауға және алмасуға қабілетті нысандар желісі (ағылш. Internet of Things).

3GPP – ұялы телефония спецификациясын қалыптастыратын консорциум (ағылш. 3rd Generation Partnership Project).

MIMO – жүйенің спектралды тиімділігін, деректерді берудің максималды жылдамдығын және желінің сыйымдылығын айтарлықтай жақсартуға мүмкіндік беретін сымсыз байланыс жүйелерінде пайдаланылатын технология (ағылш. Multiple Input Multiple Output).

AAS – абоненттік құрылғылардың орын ауыстыруына сәйкес бағытталу диаграммасы өзгеретін антенналық жүйе (ағылш. Adaptive Antenna System).

SRS-пакет – бағдарламалық қамтамасыз ету талаптарының ерекшелігі (ағылш. Software Requirements Specification).

LTE – мобильді телефондарға және деректермен жұмыс істейтін басқа терминалдарға арналған сымсыз жоғары жылдамдықты деректерді беру стандарты (ағылш. Software Requirements Specification).

WiMax Release – құрылғылардың кең спектрі үшін үлкен қашықтықта әмбебап сымсыз байланысты ұсыну мақсатында әзірленген телекоммуникациялық технология (ағылш. Worldwide Interoperability for Microwave Access).

IPTV – цифрлық кабельді теледидар операторлары қолданатын IP хаттамасы бойынша деректерді беру желілеріндегі цифрлық теледидар технологиясы (ағылш. Internet Protocol Television).

AMF – құрылғыны базалық станцияға қосқан кезде қатынауды бақылау, сондай-ақ мобильді басқару функциясы (ағылш. Access and Mobility Management Function).

SMF – белсенді белгіленген сессияларды бақылау функциясы (ағылш. Session Management Function.

UPF – 5G ұялы желісінде қолданушылар деректерін сенімді жеткізу үшін жауап береді (ағылш. User Plane Function).

UDM – абоненттердің пайдалы және қызметтік деректерін басқаруға жауап беретін функция (ағылш. Unified Data Management).

UDR – қызметтік ақпарат сақталатын деректер базасы (ағылш. Unified Data Repository).

PCF – бұл модуль соңғы буын желілеріндегі политиканы басқаруды жүзеге асырады (ағылш. Policy Control Function).

AF – қосымша немесе қолданбалы ұялы байланыс модулі (ағылш. Application Function).

NSSF – желі қабатын анықтау модулі (ағылш. Network Slice Selection Function).

PCF- 5G байланыс желісіндегі ережелерді басқару модулі (ағылш. Policy Control Function).

NEF – басқа қосымшалармен байланысты бақылауға арналған модуль (ағылш. Network Exposure Function).

NRF – барлық желілік функционал сақталатын модуль (ағылш. NF Repository Function).

SMSF – NAS хаттамасының көмегімен SMS қабылдау/жіберу үшін жауап беретін функция (ағылш. SMS Function).

NAS – деректерді сақтаудың желілік жүйесі, ақпаратты сақтаудың желілік қоймасы (ағылш. Network Attached Storage).

SMS – ұялы телефон арқылы қысқа мәтіндік хабарламаларды қабылдау және жіберу технологиясы (ағылш. Short Message Service).

STB – сандық теледидар ресивері (ағылш. Set-Top Box).

VANET – зияткерлік көлік жүйесі (ағылш. Vehicular Ad-Hoc Network).

ЖКО – жол көлік оқиғасы.

MMS – мультимедиалық хабарларды жіберу жүйесі (ағылш. Multimedia Messaging Service).

1G – сымсыз телефон технологиялары мен мобильді телекоммуникациялардың бірінші буыны (ағылш. 1 – Generation).

2G – сымсыз телефон технологиялары мен мобильді телекоммуникациялардың екінші буыны (ағылш. 2 – Generation).

GSM – уақыт пен жиілік бойынша арналарды бөлумен цифрлық ұялы байланыстың жаһандық стандарты (ағылш. Groupe Spécial Mobile).

PIN – жеке сәйкестендіру нөмірі (ағылш. Personal Identification Number).

PUK – SIM картасының жеке құлпын ашу коды (ағылш. Personal Unlock Key).

VLR – абоненттердің уақытша деректер базасы (ағылш. Visitors Location Register).

RAND – стратегиялық зерттеу орталығының функцияларын орындайтын американдық коммерциялық емес ұйым (ағылш. Research and Development).

SRES – пікір генерациясы (ағылш. Signed Response).

TDMA – радиожиілікті пайдалану тәсілі, бір жиілік интервалында бірнеше абонент болғанда, әртүрлі абоненттер әртүрлі уақытша слоттарды пайдаланады (ағылш. Time Division Multiple Access).

TMSI – мобильді абоненттің халықаралық идентификаторы (ағылш. International Mobile Subscriber Identity).

UMTS – Әмбебап Мобильді Телекоммуникациялық Жүйе (ағылш. Universal Mobile Telecommunications System).

USIM – кеңейтілген SIM карта стандарты (ағылш. Universal Subscriber Identity Module).

AUTH – белгілі бір адамға немесе тұлғалар тобына белгілі бір әрекеттерді орындауға құқық беру.

DOS – есептеу жүйесіне, оны бас тартуға жеткізу мақсатында хакерлік шабуыл (ағылш. Denial of Service).

Ethernet – компьютерлік және өнеркәсіптік желілерге арналған құрылғылар арасындағы пакеттік деректер беру технологиялары.

U-Plane – пайдаланушы деректері.

MAC – белсенді жабдықтың әрбір бірлігіне берілетін бірегей идентификатор (ағылш. Media Access Control).

AES – блокты шифрлаудың симметриялық алгоритмі (ағылш. Advanced Encryption Standard).

DES – симметриялық шифрлау алгоритмі (ағылш. Data Encryption Standard).

3G – сымсыз телефон технологиялары мен мобильді телекоммуникациялардың үшінші буыны (ағылш.3 – Generation).

NGMN – ұялы операторлар қауымдастығы (ағылш. Data Encryption Standard).

SDN – басқару функционалы пакеттерді жіберудің төменгі деңгейінен бөлінген кезде желі қызметтерін басқаруға мүмкіндік беретін компьютерлік желілерді басқару әдісі (ағылш. Software Defined Network).

NFV – телекоммуникациялық желінің физикалық желілік элементтерін виртуалдау технологиясы (ағылш. Network Functions Virtualization).

HTTP – гипермәтіндік құжаттар түріндегі мәліметтерді беру хаттамасы (ағылш. Hypertext Transfer Protocol).

C-RAN – жаңа ұяла желі архитектурасы (ағылш. Cloud-RAN).

API – қосымшаның бағдарламалық интерфейсі (ағылш. Application programming interface).

TLS – көлік деңгейін қорғау хаттамасы (ағылш. Transport layer security).

SSL – қорғалған сокеттер қабаты (ағылш. Secure sockets layer).

VMNO – ұялы байланыстың виртуалды операторы (ағылш. Mobile virtual network operator).

CSP – криптографиялық операцияларды жүзеге асыруға мүмкіндік беретін криптоправайдер (ағылш. Cryptography Service Provider).

SLA – клиенттің құқықтары мен міндеттерін анықтайтын құжат (ағылш. Service Level Agreement).

Ipsec – IP пакеттерін тасымалдау кезінде шифрлау, аутентификациялау және қорғауды қамтамасыз ету мәселелеріне қатысты хаттамалар жиынтығы.

MCC – елдің мобильді коды (ағылш. Mobile Country Cod).

IDS – басып кіруді анықтау жүйесі (ағылш. Intrusion Detection System).

Әдебиеттер тізімі

1 Omar Santos, John Stuppi. CCNA Security 210-260 Official Cert Guideб - Cisco Press, 2015

2 Сайт https://www.3gpp.org/

3 Сайт https://5g-ppp.eu/

4 3GPP TR 33.899: "Study on the security aspects of the next generation system",https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3045

5 3GPP TS 33.501: "Security architecture and procedures for 5G System - 5.2.5 Subscriber privacy", https://portal.3gpp.org/desktopmodules/Speciicatio \ns/SpecificationDetails.aspx?specificationId=3169

6 P. Kulkarni, R. Khanai, and G. Bindagi, “Security frameworks for mobile cloud computing: A survey,” in 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), March 2016, pp. 2507–2511.

7 S. S. Vikas, K. Pawan, A. K. Gurudatt, and G. Shyam, “Mobile cloud computing: Security threats,” in 2014 International Conference on Electronics and Communication Systems (ICECS), Feb 2014, pp. 1– 4.

8 A. Chonka and J. Abawajy, “Detecting and Mitigating HX-DoS Attacks against Cloud Web Services,” in 2012 15th International Conference on Network-Based Information Systems, Sept 2012, pp. 429–434.

10 Сайт https://ru.wikipedia.org/wiki/Безопасность_GSM

11 Сайт https://www.3g4g.co.uk/Tutorial/ZG/zg_security.html

12 Сайт https://www.rfwireless-world.com/Tutorials/LTE-security.html

13 N. Alliance, “NGMN 5G white paper,” Next Generation Mobile Networks, White paper, 2015.

14 3GPP. (2017, May) SA3-Security. The Third Generation Partnership Project (3GPP). [Online]. Available: http://www.3gpp.org/Specifications-groups/sa-plenary/54-sa3-security

15 ONF. (2013) SDN Security Considerations in the Data Center. Open Networking Foundation. [Online]. Available: https://www.opennetworking.org/sdn-resources/sdn-library

17 M. Liyanage, A. Gurtov, and M. Ylianttila, Software Defined Mobile Networks (SDMN): Beyond LTE Network Architecture. John Wiley & Sons, 2015.

18 M. Liyanage, A. Braeken, A. D. Jurcut, M. Ylianttila, and A. Gurtov, “Secure communication channel architecture for Software Defined Mobile Networks,” Computer Networks, vol. 114, pp. 32 – 50, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128617300075

19 R. Yu, Z. Bai, L. Yang, P. Wang, O. A. Move, and Y. Liu, “A Location Cloaking Algorithm Based on Combinatorial Optimization for LocationBased Services in 5G Networks,” IEEE Access, vol. 4, pp. 6515–6527, 2016. 2017 IEEE Conference on Standards for Communications and Networking (CSCN) 198

20 F. Kemmer, C. Reich, M. Knahl, and N. Clarke, “Software defined privacy,” in 2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW), April 2016, pp. 25–29.

21 A. N. Khan, M. M. Kiah, S. U. Khan, and S. A. Madani, “Towards secure mobile cloud computing: A survey,” Future Generation Computer Systems, vol. 29, no. 5, pp. 1278 – 1299, 2013, special section: Hybrid Cloud Computing. [Online]. Available:

22 S. Sezer, S. Scott-Hayward, P. K. Chouhan, B. Fraser, D. Lake, J. Finnegan, N. Viljoen, M. Miller, and N. Rao, “Are we ready for SDN? Implementation challenges for software-defined networks,” IEEE Communications Magazine, vol. 51, no. 7, pp. 36–43, July 2013.

23 M. Agiwal, A. Roy, and N. Saxena, “Next Generation 5G Wireless Networks: A Comprehensive Survey,” IEEE Communications Surveys Tutorials, vol. 18, no. 3, pp. 1617–1655, thirdquarter 2016.

24 T. Kumar and M. Liyanage and A. Braeken and I. Ahmad and M. Ylianttila, “From Gadget to Gadget-Free Hyperconnected World: Conceptual Analysis of User Privacy Challenges,” in 2017 European Conference on Networks and Communications (EuCNC), June 2017, pp. 1–6.

25 L. T. Sorensen, S. Khajuria, and K. E. Skouby, “5G Visions of User Privacy,” in 2015 IEEE 81st Vehicular Technology Conference (VTC Spring), May 2015, pp. 1–4.

26 J. Freudiger, M. H. Manshaei, J.-P. Hubaux, and D. C. Parkes, “On noncooperative location privacy: A game-theoretic analysis,” in Proceedings of the 16th ACM Conference on Computer and Communications Security, ser. CCS ’09. New York, NY, USA: ACM, 2009, pp. 324– 337. [Online]. Available: http://doi.acm.org/10.1145/1653662.1653702

27 Сайт http://xgu.ru/

28 Сайт https://www.cisco.com/

29 Сайт https://unlix.ru/

30 ГОСТ Р 50571.5.54-2013 «Жерге тұйықтау құрылғылары, қорғаныш өткізгіштері және потенциалдарды теңестірудің қорғаныш өткізгіштері» А.А.Каспаров, Р.Ф.Афанасьева, Е.К.Прохорова; Алматы: 2014;

31 Абдимуратов Ж. С., Мананбаева С. Е. БЖД. «Расчет производственного освещения» в выпускных работах для всех специальностей. Бакалавриат – Алматы: АИЭС, 2009.

32 СанПиН 2.2.4.540-96 «Электрлік бұйымдар, жалпы қауіпсіздік талаптары.» Суворов Г.А. (научный руководитель), Кравченко О.К., Ермоленко А.Е.; МИНТ РК: 2013;

33 Т.С. Санатова, Т.Е. Хакимжанов. Т.С. Санатова, Т.Е. Хакимжанов. «Еңбекті қорғау және тіршілік қауіпсіздігі негіздері. Радиожиілік диапазонының электромагниттік өрістерінен қорғау» - Алматы: АИЭС, 2010 - 33 с.

34 М.К. Дюсебаев, Т.Е. Хакимжанов, Ж.С. Абдимуратов «Еңбекті қорғау және тіршілік қауіпсіздігі»/оқу құралы. АУЭС. Алматы, 2012. -80 б.

35 Журнал «ENISA THREAT LANDSCAPE FOR 5G NETWORKS», 2019 - www.enisa.europa.eu.

А Қосымшасы

Core_1 маршутизаторының бапталуы

```
Router(config)#hostname CORE_1
CORE_1(config)#interface gigabitEthernet 0/0/1.100
CORE_1(config-subif)#encapsulation dot1Q 100
CORE_1(config-subif)#ip address 192.168.1.25 255.255.255.252
CORE_1(config)#interface gigabitEthernet 0/0/1.10
CORE_1(config-subif)#encapsulation dot1Q 10
CORE_1(config-subif)#ip address 192.168.1.5 255.255.255.252
CORE_1(config)#interface gigabitEthernet 0/0/1.11
CORE_1(config-subif)#encapsulation dot1Q 11
CORE_1(config-subif)#ip address 192.168.1.9 255.255.255.252
CORE_1(config)#interface gigabitEthernet 0/0/1.12
CORE_1(config)#interface gigabitEthernet 0/0/1.13
CORE_1(config-subif)#encapsulation dot1Q 13
CORE_1(config-subif)#ip address 192.168.1.17 255.255.255.252
CORE_1(config)#interface gigabitEthernet 0/0/1.14
ORE_1(config-subif)#encapsulation dot1Q 14
CORE_1(config-subif)#ip address 192.168.1.21 255.255.255.252
CORE_1(config)# interface GigabitEthernet 0/0/0
CORE_1(config-subif)# ip nat outside
CORE_1(config-subif)# exit
CORE_1(config)# int gigabitEthernet 0/0/1.100
CORE_1 (config-subif)#ip nat inside
CORE_1 (config-subif)#exit
CORE_1(config)# int gigabitEthernet 0/0/1.11
CORE_1 (config-subif)#ip nat inside
CORE_1 (config-subif)#exit
CORE_1(config)# int gigabitEthernet 0/0/1.12
CORE_1 (config-subif)#ip nat inside
CORE_1 (config-subif)#exit
CORE_1(config)# int gigabitEthernet 0/0/1.13
CORE_1 (config-subif)#ip nat inside
CORE_1 (config-subif)#exit
CORE_1(config)# int gigabitEthernet 0/0/1.14
CORE_1 (config-subif)#ip nat inside
CORE_1 (config-subif)#exit
CORE_1(config)# int gigabitEthernet 0/0/1.15
CORE_1 (config-subif)#ip nat inside
CORE_1 (config-subif)#exit
CORE_1 (config)#ip access-list standard FOR-NAT
CORE_1 (config-std-nacl)#PERMIT 192.168.1.0 0.0.0.255
CORE_1 (config-std-nacl)#PERMIT 10.1.0.0 0.0.255.255
```

CORE_1 (config-std-nacl)#PERMIT 10.2.0.0 0.0.255.255
CORE_1 (config-std-nacl)#exit
CORE_1(config)#ip nat inside source list FOR-NAT interface gigabitEthernet 0/0/0 overload
CORE_1(config)#ip route 10.2.4.0 255.255.252.0 192.168.1.14
CORE_1(config)#ip route 10.2.8.0 255.255.252.0 192.168.1.18
CORE_1(config)#ip route 10.1.0.0 255.255.252.0 192.168.1.6
CORE_1(config)#ip route 10.1.4.0 255.255.252.0 192.168.1.6
CORE_1(config)#ip route 10.1.8.0 255.255.252.0 192.168.1.10
CORE_1(config)#ip route 10.2.0.0 255.255.252.0 192.168.1.18
CORE_1 (config)#crypto isakmp policy 100
CORE_1 (config-isakmp)#encryption 3des
CORE_1 (config-isakmp)#hash md5
CORE_1 (config-isakmp)#authentication pre-share
CORE_1 (config-isakmp)#group 2
CORE_1 (config-isakmp)#lifetime 86400
CORE_1 (config)#crypto isakmp key med address 210.210.2.2
CORE_1(config)#ip access-list extended FOR-VPN
CORE_1(config-std-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
CORE_1(config-std-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
CORE_1(config-std-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
CORE_1(config-std-nacl)#permit ip 10.1.0.0 0.0.255.255 192.168.2.0 0.0.0.255
CORE_1(config-std-nacl)#permit ip 10.1.0.0 0.0.255.255 10.3.0.0 0.0.255.255
CORE_1(config-std-nacl)#permit ip 10.1.0.0 0.0.255.255 10.4.0.0 0.0.255.255
CORE_1(config-std-nacl)#permit ip 10.2.0.0 0.0.255.255 192.168.2.0 0.0.0.255
CORE_1(config-std-nacl)#permit ip 10.2.0.0 0.0.255.255 10.3.0.0 0.0.255.255
CORE_1(config-std-nacl)#permit ip 10.2.0.0 0.0.255.255 10.3.0.0 0.0.255.255
CORE_1(config)#interface gigabitEthernet 0/0/0
CORE_1(config-if)#crypto map RFT
CORE_1(config)#enable secret ADMIN
CORE_1(config)#username admin privilege 15
CORE_1(config)#aaa New-model
CORE_1(config)#aaa authentication login default group radius local
CORE_1(config)#radius-server host 192.168.1.26 key cisco

Distribution_1 коммутаторының бапталуы

```
Distribution_1(config)#interface FastEthernet0/1
Distribution_1(config -if)#switchport mode access
Distribution_1(config -if)#switchport access vlan 100
Distribution_1(config)#interface FastEthernet0/2
Distribution_1(config -if)#switchport access vlan 10
Distribution_1(config -if)#switchport mode access
Distribution_1(config)#interface FastEthernet0/3
Distribution_1(config -if)#switchport access vlan 11
Distribution_1(config -if)#switchport mode access
Distribution_1(config)#interface FastEthernet0/4
Distribution_1(config -if)#switchport access vlan 12
Distribution_1(config)#interface FastEthernet0/5
Distribution_1(config -if)#switchport access vlan 13
Distribution_1(config -if)#switchport mode access
Distribution_1(config)#interface FastEthernet0/6
Distribution_1(config -if)#switchport trunk allowed vlan 10-14,100
Distribution_1(config -if)#switchport mode trunk
Distribution_1(config)#interface range fastEthernet 0/2-6
Distribution_1(config-if-range)#switchport port-security
```